12/29/03

CPA/3621

AF

#21

2-14-04

mel

REPLY UNDER 37 CFR 1.116- Expedited Procedure –
Technology Center 3621

Khai Hee KWAN
P.O.BOX 1178
Sandakan 90713
Sabah, Malaysia

Email: khkwan@yahoo.com
Customer Number: 023336

David Q Le
Examiner
Art Unit 3621
C/o Commissioner for Patents
Mail Stop Non-Fee Amendment
P.O.Box 1450
Alexandria VA 22313-1450
USA

RE: RESPONSE FOR YOUR ACTION LETTER MAILED 29 Sept 2003 FOR CPA - APPLICATION 09/396005

Dear Sir,

In response to the above action letter, our response is as attached and consist of the following

Pages

Official Response 65

We hereby certified that this response was mailed on the 18 Dec 2003 using mailing label: EE 634529045 MY

Thank you

Yours truly,

Khai Hee KWAN

Dated 18 Dec 2003

Application number: 09/396005 **Art Unit:** 3621
Applicant: Khai Hee Kwan **Examiner:** David Q. Le
Title: Method, apparatus and program to make payment in any currencies through a communication network system using prepaid cards

Administrative Issues:

We have previously submitted our Declaration of prior Invention under 37 CFR 1.131 as part our response to final action but to date we have yet to receive any response despite querying said in our subsequent CPA application. We therefore ask the examiner again for the results to our submitted declaration in order for us to better assess the status of our submission.

The examiner had confirmed that the applicability of David (US Patent Application 2002/0073046 A1) as a reference insofar as related to disclosing subject matter in David's provisional application 60/146628 but without presenting evidence or factual findings for such conclusion. The standard required is one of demonstration is found in re Wertheim, 646 F.2d 527,537,209 USPQ 554, 564 (CCPA 1981) and not one of conclusory statement. The applicant object to the examiner's failure in fulfilling this demonstration requirement. In particular the court has made this determination where the examiner has a duty to determine which of David's parent application containing the common subject matter which would made David's claims to be patentable in order to rely on the filing date. "For if a patent could not theoretically have issued the day the application was filed, it is not entitled to be used against another as 'secret prior art' " under 35 U.S.C. 102(e)." While it is plain that re Wertheim was decided before the introduction of application publication as prior art under 102(e), there is no reason to deny well founded legal rulings.

Secondly, a continuation-in-part application relates back to its parent's (provisional) filing date for the common subject matter as in David's case extending into two provisional applications of which only one with an earlier filing date to ours, must also meet the written description requirement; by describing the claimed invention with all its limitations in addition to the presence of common subject matter. See Lockwood v. American Airlines, Inc, 107 F.3d 1565, 1571, 41 USPQ2d 1961, 1965-66 (Fed. Cir. 1997) at 1966. If said parent's disclosure merely renders the subject matter obvious for the latter filed application, then the latter is not sufficient to reach back to the parent's filing date. See Tronzo V Biomet, Inc 156 F.3d 1154, 47 USPQ 2d 1829,1832 (Fed Cir 1998). In this respect, the examiner's conclusory confirmation of subject matter disclosure is insufficient given no explanation as to the degree of said subject matter actually meeting ALL the limitations requirement.

In particular, we found no limitations describing debit card transactions, P 56, TB Server (P 85-88) or even the existence of P 85-88 and Fig 6-8 in the provisional application. It is insufficient as written description, for purposes of establishing priority of invention, to provide a specification that does not unambiguously describe all limitations. See , e.g. , Wagoner v. Barger , 463 F.2d 1377, 1380, 175 USPQ2d 85, 86-87 (CCPA 1972); Dyer v. Field , 386 F.2d 466, 156 USPQ 85 (CCPA 1967); Bocciarelli v. Huffman , 232 F.2d 647, 109 USPQ 385 (CCPA 1956).

For example, in the provisional application, only 3 objects were stated but in the subsequent later filed CIP application at page 2, 12 objects were defined or redefined. Those that we can identify word by word as common subject matter are P17 as to first para of Provisional application at page 3, P18 with second para of Provisional Application at page 3 and P 19 with third para of Provisional application at page 3. As for the purported subject matter in the Abstract, the CIP described "a user device having a finger print, a provider's server and a means for providing verification of user's identity...etc" which is totally new since David's provisional application made no mention of finger print or device means to verify finger print.

In supporting that our assertion is correct, we further applied a third party plagiarism software to determine the results as shown in Appendix 2. The principle of plagiarism is similar to finding common matter when comparing two sets of texts. Details of the software and summary are also found in Appendix 2. Comparing our manual result and from the software and where there is any discrepancy we will resolve in Examiner's

favor, the only paragraphs from David's CIP identified to have material support entitled to the earlier filing date : **P5, P 7, P10, P 12, P 17, P 18, P 19, P 22, P 23, P 25.**

Because we are unable to agree on the examiner's conclusion given the facts speak for itself, we must object and therefore will leave this issue for review later where necessary.

Status of Claims

The examiner has rejected claims 13,15,17, 19, 20-22, 24 under 35 USC 103(a) as unpatentable over David (US Patent Application 2002/0073046 A1), in view of Stimson et al, US 5577109 and further in view of Rosen (US 5455407). Although the examiner did not explicitly mentioned claims 16, 20, 25 and 14,18, 23 and 26-28 and 29-31's rejections in view to a particular section, we believe it is the unstated intention to group them under Section 103 (a) as per above.

ALL rejections are respectfully traversed with the following reasoning as detailed below.

Amendments to Claims as per this response.

Details marked changes are appended in Appendix 1. Without conceding the validity of the examiner's arguments and to expedite prosecution of the application, we respectfully ask the examiner's permission to enter the amendments as detailed in Appendix 1 (Marked version).

Our Response to the examiner's rejection.

As per Claim 13,17,22

This rejection is respectfully traversed. We have grouped all claims 13,17,22 as they have the same elements except for different classes where Claim 13 is the representative.

The examiner stated evidence from David: Abstract; Summary of the Invention: Page 2, P22; P7, P85-88: Fig 6-8, associated text; and Stimson: C2, L1-4; L25-30; L32-36; L38-39; L42-44; C3 L64-67; and Rosen: Abstract; Summary of the Invention; Fig 36 and 46, associated text).

We found that publication US 2002/0073046 A1 by David (herein refer to as CIP) has disclosed P7, P 85-88 , P 22, Fig 6-8, associated text as evidenced by the examiner. However, on comparing with the provisional application filed 30 July 1999 (David), these embodiments P 85088 and Fig 6-8 are not present and must necessarily constitute new matters unless the examiner can show otherwise (See Appendix 2). Furthermore, in order for a disclosure to be inherent, however, the missing descriptive matter must necessarily be present in the parent application's specification such that one skilled in the art would recognize such a disclosure. See Continental Can Co. USA v. Monsanto Co. , 948 F.2d 1264, 1268, 20 USPQ2d 1746, 1749 (Fed. Cir. 1991). The contention here is that there is nothing in the provisional application to suggest that other than credit cards, the use of debit cards or account identifier or user to user fund transfer are necessarily a part of the disclosure. In particular Figs 6-8 are not found in Provisional Application by David filed 30 July 1999. Para 1 of Section 112 requires exact limitations to be present in order to apply the filing date to show common subject matter.

P7 deals with online purchase and P22 deals with summary of David which we accepted forms part of the subject matter as at the earliest filing date.

P 85-88 is about debit cards which disclosed username and password however said elements are not found in the earlier filed provisional application so constituting new matter. Abstract, Summary of the Invention merely described the use of finger print in lieu, a subject matter not found in the provisional and has nothing to do with our claims. The original application deals with ISP's assigning an IP address and for purchases with online merchants while our claims 13,17, 22 deals with user to user fund transfer. A reading of the provisional application specification demonstrates the usage of credit card with an ISP model only and nothing broader contrary to the examiner's assertion.

However, password is identified in Fig 3, 4 of David's provisional application but its usage is in confirming a purchase rather than as disclosed in our application to authenticate the payer's account for validity ie prepaid account being linked to user account identifier in the database. See Fig 3 where it asked the user for confirmation of the purchase which is followed by Fig 4. David's uses an ISP model so its common in the art to have this step to access the ISP's services but this does not reach our claim where we are authenticating the validity of a linked pre-paid account rather than ISP services. Even if we count this as one element, the other element of user name is new matter found only in the CIP. David's provisional uses Buyer ID Code (Pg 9) and it is generated by the buyer's computer (David Pg 9) which does not show our self created account identifier as shown in Claim 13 & and self creation part in 14.

As previously noted Fig 6-8 of David's later application are not found in the earlier provisional application and therefore are new matter without the benefit of the earlier filing date contrary to the examiner's assertion. If the figures are not in the provisional application then it is only reasonable to assume that the specification could not reveal the details and hence the limitations of said figures. See Lockwood v. American Airlines, Inc., 107 F.3d 1565, 1571, 41 USPQ2d 1961, 1965-66 (Fed. Cir. 1997). Section 112, paragraph 1 requires that the specification "contain a written description of the invention, and of the manner and process of making and using it ... ." To meet this requirement, the disclosure of the earlier application, the parent, must reasonably convey to one of skill in the art that the inventor possessed the later-claimed subject matter at the time the parent application was filed. See Vas-Cath Inc. v. Mahurkar , 935 F.2d 1555, 1563, 19 USPQ2d 1111, 1116 (Fed. Cir. 1991); see also Hyatt v. Boone , 146 F.3d 1348, 1354-55, 47 USPQ2d 1128, 1132 (Fed. Cir. 1998). A disclosure in a parent application that merely renders the later-claimed invention obvious is not sufficient to meet the written description requirement; the disclosure must describe the claimed invention with all its limitations. See Lockwood , 107 F.3d at 1572, 41 USPQ2d at 1966. It is clear that these limitations in Fig 6-8 were not meet as not all the limitations are found in the provisional application. With missing limitations, the Figs 6-8 and hence associated text would not necessarily convey to one skilled in the art that the David actually possessed the claimed subject matter as at filing date 30 July 1999. (See Appendix 2 for details)

The examiner further stated that Stimson directs itself to debit cards while David's credit card transactions, however, in this particular claim neither are sought directly as the stored funds are already in the database. The examiner provided the following evidence; C2, L1-4; L25-30; L38-39; L42-44; C3 L64-67 which are reproduced in full below:

At C2, L1-4 reads " It is still another object of the invention to provide a pre-paid card system and method that facilitates point to sale activation of cards using data terminals connectable to a host computer" ; L25-30 reads " It is still a further object of the invention to provide a pre-paid card system wherein the host maintains a database of authorized cards, the database including detailed information about the authorization, recharge and use status of each card in the system"; L38-39 reads "..cardboard or plastic and may include the security number in cleartext under a suitable blackout. The main management..." ; L42-44 reads " ...host computer, which is connectable to the telephone network. The host computer includes a database for storing security numbers associated with authorized calling cards. The data terminals are...";

and C3 L64-67 reads " ...therein a security number. The card is typically formed of cardboard, paper or plastic and many include the security number in cleartext under a suitable user-removable scratch-off or other material 22 (such as an opaque tape). If desired.."

Claim 13 simply shows the method of transferring pre-stored fund in a database at a server by payer to payee applying account identifiers. Neither Stimson and David has this feature and while Stimson shows a debit card linked to an account and a prepaid card with stored value, there is no combinable features evidencing them to reach transferring of the stored value to another user by way of an identifier account. The examiner did not specifically state what is it in David to combine with Stimson to reach our claim given neither expressly mentioned account identifier. This is not the same as saying Stimson teaches an account in a database stored with the prepaid card code as our account identifier uses the user's own chosen identifier which is further linked to the first stated account. To show obviousness to one skilled in the art in view of Rosen, there must be some basis in Stimson to show desirability to create an account identifier from an account and linking it with pre-stored funds. None was evidence.

In short, Stimson and David have to show a payee's identifier account known to the payer to effect the transaction, none of which are disclosed in said prior arts. Perhaps more importantly is the logic behind Stimson where the 'account' actually shows the secret code in the prepaid card which one skilled in the art would recognize should not be given out to anyone or known to another even for the express purpose of transferring funds by another. The difference here relates to the account in Stimson and our account identifier, the latter is to promote fund transfer and its created by linking the code in the prepaid card and a chosen password and appropriate storage period, currency etc. Once an account identifier is created the code on the prepaid card is of no value in our claim.

In Stimson the code in the database and the code in prepaid card is persistent and is created by prepaid card service provider and not of user's own choosing and cannot be modified. The code is for authenticating the card, payment and for activation (adding of funds) by user. There is no other 'alias' or identifier to link to the secret code in Stimson. Any third party knowing this code can use the card for mischief while in our account identifier, it requires a further a password and hence knowing the identifier alone is insufficient which makes it a good substitute to the codes for fund transfer. Stimson's teaching is to preserve the card for future transactions including reusability through reactivation which is the novelty of his invention. It is obvious that Stimson is not aware of our problem and in particular the issue for user to user fund transfer could not be found in his teaching (reading the difference as a whole). As stated in In re Zurko, 111 F.3d 887, 42 USPQ2d 1476 (Fed. Cir. 1997), the nature of the problem cannot be used as motivation when the problem had not been previously identified anywhere in the prior art.

Furthermore in this claim, funds is assumed to be pre-stored first in the database while Stimson's card has to be activated first and the transfer is instantaneous which is not possible in David's case where it is clear a credit card has to be billed by the ISP later and be paid even later through the normal bill presentment process. As we mentioned, David only mentioned Debit Cards in his later filed applications and not entitled to the earlier filing date. This means the Examiner has to additionally show why David in view of Stimson should find it desirable to use a Debit Card which is not evidenced.

In Rosen, the examiner directed us to review evidence Fig 36, 46 and associated text.

The examiner showed Rosen Fig 46 as evidence of obviousness to reveal foreign currency. We beg to disagree with the facts provided. The Fig shows two different parties buying and selling currency or commonly known as a foreign exchange transaction which is not what we are claiming. In the first instance the payee is not conducting a foreign exchange transaction with the payer as in a buy/sell foreign currency situation. Our claim calls for fund transfer in any currencies and not in the buying or selling of any currencies which is not the same nor inherent as the latter requires two parties to interact with each other to

decide on the appropriate exchange rate on a willing buyer and seller basis. In our instance, the payer wish to transfer funds to payee in a particular currency where the payee is not obliged to 'buy' or 'exchange'. In fact, the process of fund transfer is not a buy or sell transaction unless the examiner can show this inherency to anticipate this element. None was evidence.

Our claim shows its merely a transfer of funds to another party and the exchange rate is decided by the server where the payer only has to agree or reject which has no interaction with payee at all. Furthermore as we shall discuss below, this is a one sided transaction without interacting with the other party (payee) unlike what Rosen has taught involving two parties negotiating on the exchange rate to sell currency to each other (reading the difference as a whole). To show one skilled in the art would expect reasonable success the examiner need to reason how to reach transferring funds in any currencies stored in a database without interacting with payee from Rosen in view of no knowledge of our invention. Nothing so far has been evidence.

By default, the Examiner had implied that the mere disclosure of an foreign exchange mechanism between a buyer and seller, in general, via modules would render obvious the expression of any fund transfer in any currencies in the same way, even where the specific transfer is structurally and methodically different that one of ordinary skill in the art would be hard-pressed to determine how to modify to show without interacting with payee. This unstated 'obvious to try' approach seems inadequate to resolving such differences and its not the standard for a 103(a) rejection.

The examiner showed us the applicability of Rosen Fig 36.

Figure 36 reveals a subscriber to subscriber funds transfer method using money modules, however it is clear that both subscribers are actively interacting with each other in the whole process which is contrary to our claim for non-interaction with payee under payer's control.

The examiner further stated that in Summary of the Invention by Rosen suggest an automated process provided by pre-configuring hardware and software. Our reading shows that this is an assumption made by the examiner since there is no evidence in Rosen's summary to actually teach this pre-configuration process. Rosen may have wish for an automated system (Col 2 line 5) but there must be teaching so to enable one skilled in the art to implement this automation process and not simply whether one skill in the art would have been able to pre-configure the software to achieve automation process as suggested by examiner. It is well established that the standard of obviousness is not whether one skilled in the art is capable to arrive at the claimed invention. See Ex-parte Levengood, 28 USPQ 2d 1300 (Bd Pat App & Inter. 1993)

In particular the evidence alluded in Rosen Summary, the money module reads as "The invention comprises a money module for generating the electronic money; a money module for issuing, distributing, and accepting the electronic money; and a money module for accepting, storing, and transferring the electronic money between other accepting money modules and between the accepting money module and the issuing money module."

In Col 8, line 39 – 51: it is written by Rosen "As will be appreciated, the Transaction money module 4 may be configured to make deposits, withdrawals, loan payments, inquiries and exchanges of currencies of electronic notes 11 directly through a Teller money module 5 at an Issuing 1 or Correspondent Bank 2 or remotely through a telephonic connection to an Issuing 1 or Correspondent Bank 2 Teller money module 5 (thereby providing, among other things, the transactions not available in current home banking systems).

Upon a request to transact with a bank, the Teller money module 5 mediates the transactions for the subscriber's bank account as well as the banking system's electronic money accounts. "

However, this is no fully automation process by way of pre-configuration as suggested. The reading only show that the money module can be configured or designed to make deposits etc just like any software program can be programmed by inserting codes to perform certain function but by itself there is no teaching that it could handle said functions automatically without any intervention by payee. Rosen had compared this to then home banking system which cannot actually make deposit or withdrawals. In short his innovative modules are like 'electronic wallets' with Electronic Money (drawn on deposit claims) capable of making transfer at will to other subscriber's modules. (Note Rosen's teaching is a divisional filed in 1991.)

This finding of automation by pre-configuration, however, was unsupported by substantial evidence because it was based on the Examiner's unsupported assumption, or alternatively, unsupported finding, as to the third Graham factor: the difference between the prior art and the claims at issue, as viewed from the vantage point of one of ordinary skill in the art. The Examiner's decision reveals its implicit assumption that one of ordinary skill in the art would have perceived the difference between the disclosed module to module payment and payment without interacting with payee to be insignificant and can be substituted by a pre-configuration process well within the capability of one skilled in the art. Even assuming that this implicit assumption constituted an actual "finding" by the Examiner, it was unsupported by any evidence, let alone substantial evidence, that one of ordinary skill in the art would have agreed that the mere disclosure of user to user payment module system in Rosen would have led one of ordinary skill in the art to believe a reasonable degree of success could similarly be expected by pre-configuring it. "The consistent criterion for determination of obviousness is whether the prior art would have suggested to one of ordinary skill in the art that this process should be carried out and would have a reasonable likelihood of success, viewed in the light of the prior art." In re Dow Chem. Co., 837 F.2d 469, 473 (Fed. Cir. 1988).

It is well known in the art that some form of interacting is required as shown in Fig 36. In fact, our reading of col 49 and 50, shows extensive interaction between payer and payee starting from signing on (steps 10-42) at the same time and to issue an entitlement to receive payment (steps 808 & 812) by payee and verification/acceptance by payee (step 830 & step 832). For example if payee does not know when payer is going to sign on the system to effect a transfer (effectively without payee's intervention) then subsequent steps will not occur. Hypothetically, even if all these interactive steps can be pre-programmed, there still would be a requirement for both payee and payer to co-ordinate these steps off-line within their respective modules in order to 'automate' the process. For example knowing when both parties are to sign on.

Furthermore, assuming there is no interaction with the human payee directly, there is still interaction with the payee's program (module) embodying the steps pre-configured by payee. In short, in Rosen's teaching there is a need to interact between the two modules either by their human handlers or pre-configured by the human handlers if indeed taught by Rosen to pre-configuring it. Therefore, to combine with Rosen to show user to user without interacting with payee, the examiner has to further evidence that payee's modules are not required at all. This is a significant difference between the claimed subject matter with Rosen as a whole from the vantage point of one skilled in the art and could not be simply be substituted by reasoning "pre-configuration" without substantial supporting evidence.

Furthermore, what is the motivation to switch from a module system to a centralized system and to apply pre-stored funds instead of claimable deposit funds in the form of E-M stored in modules ? Rosen specifically speaks about issues connected with a centralized system linked to the banking network using credit and debit cards and his solutions is to use modules. (Col 1 line 65- Col 2 line 4). The examiner clearly also relied on the unstated assumption that the difference between pre-stored funds in a database and electronic money stored in a module is insignificant which is misguided as the difference here also reflected

the significant structural difference between our claim (using a database) as a whole and Rosen's teaching (using modules).

In our claim, there is no payee interaction or payee's module but merely a transfer to payee's account in the database executed by payer through payer's account. In fact what is claimed is a payer doing all the executable without interacting with payee. It is clear that we do not use a payee module which is the critical structural difference not obvious. In our claim, the Payee has an account identifier wherein linked to a money account are ascribed in a database whereby the account with the pre-stored funds is stored in a server. In Rosen, the money modules are embedded in respective subscriber's devices (See Fig 3) and are personal to each subscriber allowing only the said subscriber access. The actual transfer is done by the transaction module which is a sub component of the money module. These modules are identified by the network destination number and not a user identifier of ones own choosing. Rosen taught the subscriber's account identifier ('as a serial number') to be one fixed in the module by issuing bank or module provider and its never changed (Col 12 line 30-33) and as an example, Rosen pointed to applying this serial number in the form of a subnetwork as identifiable by the local network 16,17,18. (Col 18 Lines 11-19). In short, this identifier is not chosen by the user but allocated by the service provider (bank) under its various network protocol similar to IP addresses (60.111.11.1). Given an IP address is usually by assignment by system admin, one skilled in the art of network protocol would not be able to see obvious that this identifier could be a name or a number of choice. While a domain name server (DNS) could theoretically be installed to reverse map to a domain name, it is not well known to do so for a user to user payment system. And even if this could be obvious, it still does not structurally meet our claim where such identifier cum password are stored in a database and not in a module.

The examiner must similarly shows that Rosen discloses a single module operated or pre-programmed by payer (NOT PAYEE) to automate the whole process to satisfy the no interacting with payee limitation. At the very minimum, Rosen has to show that funds transfer is capable by using a single module and not two modules interacting with or without a human payee handler.

The examiner continued by suggesting that said automation process is inherently means no intervention by payee. To rely on inherency to establish the missing features " no intervention by payee ", case law in *Ex parte Levy*, 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990) requires the examiner to provide a basis in fact and/or technical to support this. None was demonstrated and neither did the examiner show how this automation is structured or done to reveal non intervention.

We also further submit that " no intervention by payee " as asserted by examiner does not necessarily show " no interaction with payee " as claimed. The operative word is WITH and not BY as suggested by examiner. For instance, no intervention by payee could mean that the payee is aware of a fund transfer and have configured his or her module in anticipation but provided no intervention during the actual process itself. This is a logical assumption since the examiner supports this 'no intervention' by collaborating it with pre-configuration whereas "without interacting" means not even pre-configuring and no knowledge of a fund transfer to satisfy no interaction with the payee at all.

In touting automation by pre-configuration to assume no intervention, the examiner merely pointed out "Summary of invention" by Rosen which made no such suggestion. We have reproduced the entire Summary below for factual finding in quotation marks.

"In accordance with these and other objects of the invention, a brief summary of the present invention is presented. Some simplifications and omissions may be made in the following summary, which is intended to highlight and introduce some aspects of the present invention, but not to limit its scope. Detailed descriptions of a preferred exemplary embodiment adequate to allow those of ordinary skill in the art to make and use the inventive concepts will follow in later sections.

According to a broad aspect of the invention, an electronic monetary system provides for transactions utilizing electronic money including electronic currency backed by demand deposits in a bank in lieu of cash transactions, and electronic credit authorizations. The invention comprises a money module for generating the electronic money; a money module for issuing, distributing, and accepting the electronic money; and a money module for accepting, storing, and transferring the electronic money between other accepting money modules and between the accepting money module and the issuing money module.

According to a further aspect of the invention, an electronic monetary system is provided for implementing and maintaining electronic money which includes electronic currency that is interchangeable with conventional money through claims on deposits in a bank and electronic credit authorizations.

The system includes a plurality of issuing banks; a generator module for creating electronic money; teller modules coupled to the generator module, for performing teller transactions and for interfacing with other teller modules, such transactions including the accepting and the distributing of the electronic money; a security system for providing the overall integrity of the electronic monetary system; a clearing and settling process for balancing the electronic money accounts of the separate issuing banks and for clearing the electronic money issued by the issuing banks; and a plurality of transaction modules owned by authorized users, for transferring the electronic money between the transaction modules and between the transaction modules and the teller modules.

In accordance with another aspect of the invention, the functions of the generator modules, the transaction modules, and the teller modules will be performed by a combination of tamper-proof computer hardware and application software that may be networked together.

The electronic money exchanged by these modules, which may be an electronic representation of currency backed by demand deposit accounts at the issuing bank or credit authorizations, may be transmitted with digital signatures to provide security from unauthorized modification or counterfeiting. In a preferred embodiment, security from counterfeiting and tampering is also provided by requiring the modules and the individual units of electronic money to be renewed periodically. Offending modules or counterfeit electronic money can be removed from circulation as soon as they are discovered.

Briefly, a process in accordance with the invention comprises the steps of

(1) providing a generating module to generate electronic representations of economic value backed by demand deposits or by a credit line;

(2) providing a teller module to accept the generated electronic representations of economic value and to issue the electronic representations of economic value;

(3) providing the authorized users with a transacting module for accepting, storing and transferring the electronic representations of economic value to other authorized users having the transacting module and to the teller processing module;

(4) accepting and transferring the electronic representations of economic value to other authorized users having a transacting module and to the teller module; and

(5) providing a security system to allow the transfer of electronic representations of economic value in a secure manner between the generating module, the teller module and the transacting module. "

Inherency cannot be established by probabilities or possibilities. The mere fact that a certain thing (pre-configuring) may result from a given set of circumstances is not sufficient. (In re Oelrich, 666 F.2d 578,581,212 USPQ 323,326 (CCPA 1981) (quoting Hansgirg V Kemmer, 102 F.2d 212, 214, 40 USPQ 665,667 (CCPA 1939)) (emphasis added). Thus, inherency permits in limited circumstances, to gap minor but well known features or functions as seen by one skilled in the art. We are doubtful here that the suggestion by the examiner to automate the process by pre-configuring must necessarily exist or a minor feature or well known in the art of user to user fund transfer, particularly when Rosen explicitly taught payer interacting with payee using tamper proof hardware and software incorporating above said functions. As mentioned, we also could not identify any specifics in Rosen's teaching as evidenced by the examiner to reveals pre-configuration step.

And even if the whole process can be 'fully automated' as claimed by the examiner, there is still interaction between payer's module and payee's module minus their human handlers because this is what Rosen has taught. We should also reiterate the fact that in addition to "without interacting with payee", this element also supports the pre-amble whereby the transfer is wholly under payer's control hence breathing life and meaning to the preamble. We are doubtful that is would be practical under Rosen' s teaching evidencing a need for both parties to interact even in an automated form.

Even if technically this could be done, motivation is one spring from desirability viewed from one skilled in the art. Based on Rosen's teaching, we are certain that the payee would not want the payer to have control over his or her money module even if it is only for receiving funds into his account. The risk outweighs the benefit.

As mentioned in Rosen, its transfer method is only for electronic money (economic representation such as bank notes) being backed by credit or claims on deposits and the real money is settled by way of inter-bank clearing and settling. (Col 4, line 15-19) In our claim 13, the funds are transferred instantly because they are already stored and are not claims to an external account or credit line. Being a book entry, there is no dependence on the primary clearing method in the banking system. Although the examiner did not explain this point, we are doubtful said settlement is instantaneous given the need to utilize inter-bank clearing later of claimable deposits as taught by Rosen. Therefore, we distinguish Rosen as the subject matter does not involved prepaid funds to a service provider and without interacting with payee and wholly under payer's control. As mentioned, David's credit card settlement with merchant is also done off line by ISP and both David and Stimson made no teaching on user to user fund transfer.

The Motivation.

For a 103(a) rejection, not only must all elements be accounted explicitly or inherently but a motivation be found so one skilled in the art would find it obvious to combine. The examiner states "It would have been obvious to one ordinarily skilled in the art at the time the invention was made to combine the features and capabilities taught by David, Stimson, and Rosen to provide a secure, convenient, and highly desirable electronic transaction system for users of credit, debit, and prepaid cards on a global, worldwide basis."

In arriving at the stated motivation, the examiner did not explicitly state which features are being combined except for David showing credit card (which we did not claim) and Stimson shows debit/prestored card and Rosen shows currency and user to user modules. What feature in Rosen's teaching is desirable or David's teaching show secure etc ?.

The applicant respectfully submit that all the cited prior art systems possess "secure, convenience and desirable" features individually and these features are common in payment/transfer systems and so well known that on their own, one skilled in the art would not find it desirable to "re-invent the wheel" as suggested here by combining.

Arguing that the motivation to combine the references arose from the references themselves, as well as the nature of the problem to be solved, the examiner had yet to show the problem found or the teaching in Rosen in order to combine with stored value in a database and neither did Stimson show it is desirable to transfer funds to another user to reveal our solution of using self-created identifiers in lieu of security code account stored in database.

Except for Rosen, none of the other prior arts actually address this issue as found in our claimed invention in Claim 13 which is for fund transfer between users using account identifiers. However, Rosen uses money module system which identifier is pre-determined in a network but its also highly interactive using claimable deposits to back up the issued electronic money. This is not what we are claiming and the significant difference is where there is no interaction with payee contrary to Rosen teaching of a highly interactive process.

The question is why would one skilled in the art in view of David's merchant payment solution using a credit card collaborating with a friendly intermediary reach out to a prepaid/debit solution and further to a user to user transfer using modules ?. There is no mentioned of any problem with the card that is obvious to adapt it for a prepaid card in David.

David must at least teach a reason to extend to using a pre-paid card which is not found in the provisional application. As mentioned paragraph 85-88 in David CIP do not exist in the provisional application as required under 112 Para 1 meeting its limitation requirements. Stimson also did not teach "user to user transfer" using prepaid cards but only that prepaid cards for purchases to merchant. Why would one skilled in the art find it desirous to provide user to user fund transfer in view of user to merchant facility ? Simply having Rosen's Fig 46 & 36 are not sufficient unless there is teaching found in all the arts to combine the missing elements.

As the examiner mentioned the 3 features above, we will examiner each one in turn below.

Convenience.

The examiner did not reason how having to use a credit card or a debit card or a prepaid card can be convenient when the alternative may be better serve by having one type of card capable of being used in the 3 systems. In short, one would argue it is more convenient to use a credit card which is also a debit card and a prepaid card all in one whereby giving the user the choice of transaction. This suggestion of using all type of cards however is not found in all the prior arts in particularly Rosen which opted for claimable deposits.

If the examiner is suggesting the motivation is to build an universal transaction system then such motivation is not found in any of the prior arts either as it is well known that different payment instruments exhibit different system features to accommodate novel business characteristics. We do not know of a single universal system based on a single payment source. If there are such a system, it is most probably a modular combination of the various popular payment sources as disclosed separately in the prior arts.

Furthermore, our claim is not towards using a credit card or debit card but one of a stored funds for user to user fund transfer. From the vantage point of one skilled in the art, the motivation to combine is a result of desirable features found separately in view of the prior arts but advantageously when combine.

But more pertinent is that none of the prior arts actually suggest using the three payment instruments in a single system to reveal convenience and implicitly saying these prior arts are not convenient as view by one

skilled in the art. It is also odd to see that if the three prior arts are to be combined then, claimable deposits in a module should also be included but was not, suggesting that the examiner selectively pick the elements by hindsight to 'try' to meet our claim which is not permissible despite the fact that we did not claim a card of any type here.

In fact, would it not be more convenient not to use any cards at all and instead use Rosen's modules say embedded in a mobile device ? A module system effectively means no cards which is contrary to the examiner's suggestion of using 3 type of cards. Furthermore, as long as there are funds in the module, it can be used whereas with cards, one still need to ascertain if the credit limit is breach or as in the case of a debit card to check if the bank account has funds etc. By using a module, the user can check instantly instead of having to pull out each card for checking, a more burdensome task.

As we mentioned, Claim 13 is for user to user fund transfer using account identifiers with stored funds and not about using cards. In fact the word "card" does not even appear in claim 13 but rather we are claiming stored funds. We are unsure how this was neglected in determining the motivation factor, without which would not have meet our claim at all. In view to the claim as a whole, this significant difference was not appreciated when providing the motivation as neither David in view of Stimson's teaching of cards can provide a reason to bridge into Rosen's non-card system albeit not having "not interacting with payee".

The trend as disclosed in our specification and read with this claim is towards convenience and fund transfer for users. Rosen adequately describe this issue but uses a different approach whereby modules are employed interactively. There is nothing in Rosen to show that interacting between modules is not convenient and hence would trend towards non interactivity with payee as a more convenient obvious as seen from one skilled in the art.

And from Rosen's reading, why would one skilled in the art modified Rosen's system using modules and deposit claims to one without payee module or without interacting with payee and wholly under payer's control ? Also would one skilled in the art sacrifice security for convenience ? As we mentioned, Rosen's system is highly interactive between payer and payee would be more secure.

Security

As for security which is more substantive as compare to convenience or desirability as view from one skilled in the art, we submit that credit cards are not as secured as stated in David which prompted his ISP method. Similarly debit cards suffered from the same being linked to a bank account. As prepaid card as in Stimson depends on security code on the card, it shares similar fate if lost or stolen or intercepted as debit cards or credit cards. Given all cards share similar security risk, we are unsure why the examiner states the a system using the three would be secure or desirable enough to motivate.

If in fact the examiner is trying to reach our claim which uses Account Identifiers and not any cards, then security would be less secured than as compare to Stimson's prepaid card. It is well known in the art that a randomly generated code is more difficult to crack then an user identifier of user's own choosing and a password. By suggesting the use of cards the examiner not only cited a poor motivation by assuming that by using 3 different types of cards is secure but also misses the limitation of our claim of using an account identifier in lieu of cards whereby security is questionable.

Rosen actually uses digital certificate in its module and encryption which would be more secure during transmission and the same with David's encryption in the latter filed application. Given the structural difference, there is no evidence to show that a pre-stored funds in a database is more secure than using

Rosen's modules or that Rosen's modules are less secure to motivate so. Finally, why would one skilled in the art cite security as the motivation to reach our claim knowing full well that account identifiers having simple and convenient passwords would be easier to crack than a randomly generated code found in Stimson's prepaid card ?

Furthermore as we asserted, Rosen did not teach a fully automated system control by payer and without interacting with payee, the difference as a whole not obvious here. Rosen teach a highly interactive method with both payer and payee. The issue of pre-configuration is one extended by the examiner and not found in Rosen. Even if it is, Rosen still requires both payer and payee modules to electronically interact since the actual electronic money is stored in these modules, without either one, the transfer will not work.

The desirability of the Combination.

In short there must be a motivation for David and Stimson to combine with Rosen to reach a user to user transfer system and a motivation in Rosen to move to a system without interacting with payee. It does not appear the drive or motivation could simply be for a universal transaction system or that said combined system is secure, convenient or desirable given these are readily found in each of the existing systems.

And as far as the applicant is aware, there is no such system that is capable of accommodating all three systems given the significant differences underpinning their novel business, technical and accounting features. For example, we cannot used a credit card and book it under a debit card system nor can we use a debit card through a system that is designed for prepaid. To suggest combining all the payment instruments jointly in a system while maintaining their unique features (credit, debit and prepaid) seems odd technically and from a business case. For example, if the service provider is offering a credit facility then fees are made from the credit while in a debit facility a fee is deducted from each transactions and in a prepaid, a service fee is added at the time of sale of the card. Not to mention that in prepaid the amount can be deducted instantaneously, for debit card it is usually within 24 hours and through a clearing network like SWIFT if it is inter-bank and for credit card it is only billed periodically. None of these process are technically combinable in a single system nor is it desirable to do so as seen from one skilled in the art.

Else, this would explicitly mean having the teachings of the 3 prior arts programmed in a black box merely to evidence that the black box is capable of running the 3 solutions and one skilled in the art would find it desirable to fit them in simply because said black box is capable of these offerings. While technically it is possible to do so by offering these programs, we find this motivation on a balance of probability to be less persuasive as it does not really reach our claim.

The current trend is to use one single card that is capable of being serviced by the 3 systems. New cards such as those with a smartchip can store all three in one and provides the user the choice from which account the user wish to utilize for a transaction. However this does not mean the 3 systems are combinable at the back-end, all it means is that it allows the user to decide which type of transaction to be used.

If the 3 type of services (ie credit, prepaid and debit) can go through a singular system then admittedly there is a challenge but there is no teaching from any of the prior arts to show how this can be done nor are we claiming such. By merely wanting to use three type of cards by itself to provide the motivation to combine does not render our claimed invention obvious as per claim 13 since the examiner did not explain how these the different back systems and hence the governing business rules will be integrated. To do so would mean developing or rewriting an entirely set of business rules combining credit/debit/prepaid features to satisfy the three business practices jointly, a subject matter which is outside the scope of our claim here and one skilled in the art of funds transfer.

Turning the motivation on its head, one skilled in the art is faced with only two possibilities ie 1) to develop a new set of business rules to accommodate all the three type of cards while ignoring money modules in a single system or 2) physically adapting the three systems in a black box so that it will show able to use three type of cards and ignoring money modules, we are doubtful the artisan being aware of security, convenience and desirability would be so motivated given no teaching to combine each other features. As for (1) the issue of success is a concern and (2) by running 3 systems in a black box is equivalent to re-inventing the same wheel, a task that do not reveal further desirability, security and convenience.

Furthermore, neither is Claim 13 about cards but on stored funds in a database as the starting point and without interacting with payee. Only in Claim 14 do we claim a card being linked to account.

Conclusion

Hence it would not be obvious to combine three different systems designed for different problems unless impermissible hindsight was used to reach our claimed invention noting also that the examiner did not include any of Rosen's user to user feature in resultant combination. Accordingly, applicant submits that Claims, 13,17,22 are patentable over David (for subject matter found in provisional application as per 112 Para 1) in view of Stimson and further in view of Rosen given what is known in the art.

Secondly, the Examiner failed to determine (1) the difference including structural, if any, between the prior arts and the claims at issue as perceived by one of ordinary skill in the art, and (2) whether that difference, if any, is so insignificant that one of ordinary skill in the art would entertain a reasonable expectation of success in expressing " without interacting with payee in an user to user fund transfer process using account identifiers". The sum of this failure means that the Graham factors were not apply properly in determining an obviousness rejection and hence also failed to establish prima facie.

Thirdly, we also submit there is no evidence to show or teach combining the features found in the prior arts to reveal our claim at issue, if it at all reveal our claim. As we mentioned, the essence of user to user transfer without interacting with payee is missing and the motivation provided "secure, convenience and desirable" can only be surmised as opportunistic since if not all fund transfer or payment system must necessarily have such properties in order to even be considered. We would not agree that re-inventing the wheel can support adequately the motivation to combine. Accordingly with the examiner's stated motivation, there is no evidence it is 1) combinable with Rosen 2) and the using credit/debit/prepaid cards would reach our claim of using account identifiers without interacting with payee since we did not claim cards in Claim 13.

Fourthly, it is clear that not all the elements have been meet explicitly and inherently as detailed above.

Accordingly, we respectfully ask the examiner to allow these claims.

As per Claims 14, 18, 23

We respectfully transverse this rejection.

The examiner asserted " David in view of Stimson and Rosen disclose all the limitations of claims 13 and 22. " but made no mentioned of claim 17 ? We are unsure if this is a typo or intentional at page 6 of Action Letter. Claim 14 is dependent on 13, claim 23 is dependent on 22 and our claim 18 is dependent on 17.

The examiner further asserted that Stimson discloses how a debit card may be activated and discloses the following limitations of claims 14, 18, 23 by evidencing from Stimson; C2, L1-4; L25-30; L38-39; L42-44; C3 L64-67 which are reproduced in full below:

At C2, L1-4 reads " It is still another object of the invention to provide a pre-paid card system and method that facilitates point of sale activation of cards using data terminals connectable to a host computer" ; L25-30 reads " It is still a further object of the invention to provide a pre-paid card system wherein the host maintains a database of authorized cards, the database including detailed information about the authorization, recharge and use status of each card in the system"; L38-39 reads "..cardboard or plastic and may include the security number in cleartext under a suitable blackout. The main management..." ; L42-44 reads " ...host computer, which is connectable to the telephone network. The host computer includes a database for storing security numbers associated with authorized calling cards. The data terminals are..."; and C3 L64-67 reads " ...therein a security number. The card is typically formed of cardboard, paper or plastic and many include the security number in cleartext under a suitable user-removable scratch-off or other material 22 (such as an opaque tape). If desired...."

We have grouped all claims 14,18,23 as they have the same elements except for different classes where Claim 14 is the representative. As we have provided above, claims 13,17, 22 are allowable and hence the dependent claims should also be allowed. The following response is based on the claims 14,18,23 own merits which the applicant is confident of being non-obvious over Stimson.

Furthermore, despite having almost exact limitations except for "linking to an user account identifier" in preamble and an additional element " if said user account identifier, password combination is not unique and stored value is acceptable to user then linked the stored value amount to said existing user account identifier and password in the database" as compared to our immediate previous amendment, the examiner in this occasion did not provide any evidence this time to met these limitations below:

....stored period and currency;
...calculating the stored value;.
...output stored value to user;

whereas previously the examiner cited obviousness given that international transaction system would required a step of inputting currency and confirmation citing that it would be attractive and useful as per page 6 of Final Action Letter mailed 25 March 2003 (herein "Final").

We find this missing obviousness determination odd and we have to assume the unstated obviousness as the same as per Final Letter mailed 25 March 2003.

Turning to the respective elements, the applicant disagrees that Stimson shows the following elements;

" Linking to an user account identifier; "

"Determining if any identifier account is associated with the security code;"

"If there is no account identifier associated with said code then prompt user to enter a unique user account identifier, password, storage period and currency to be stored;"

"Determining said user account identifier and password for uniqueness against other stored user account identifiers and passwords;"

"Calculating the stored value;"

"Output stored value to user; "

"if said user account identifier, password combination is unique and stored value is acceptable to user then add said account identifier and password into database linked with the stored value amount; and"

"if said user account identifier, password combination is not unique and stored value is acceptable to user then linked the stored value amount to said existing user account identifier and password in the database. "

As mentioned previously the examiner's evidence did not show any steps for activating or recharging the prepaid cards. The actual detailed steps taught by Stimson is found in Col 5 line 65 to Col 6 line 14 and are reproduced below.

The following is a typical card activation or recharging scenario. Assume a customer comes up to the counter and requests $12 worth of calling time. The clerk then obtains the next calling card from the plurality of cards, and begins the activation process. This is achieved by pressing the "Sell New Card" key (1). The new card is then swiped through the card reader slot. The amount of the transaction is then entered on the keypad. At this point the terminal dials out via the modem and waits for an answer. After communicating with the host, transmitting the request, the card and terminal identifiers, and receiving a verification, the unit displays a suitable response message. The operator is then prompted to collect the funds and this message (e.g., by a message, "Done Collect $xxx.xx") tells the operator that the security number on this card has been activated for the amount shown. The transaction is completed by giving the card to the customer.

As one can appreciate, there is a significant difference between linking an account identifier to a prepaid card's amount and merely activating a card with the amount requested as per Stimson.

For example, firstly account identifier must exist or could be created by choice. In particular the step "Determining if any identifier account is associated with the security code" is not meet because Stimson has not taught of creating any identifier account in the database. Stimson merely states the database is stored with security codes from the authorized cards.

Stimson also taught that the cards have ROM strips 20 capable of storing security number whereby said security number can be user account number, a PIN etc. (Col 6 line 29 to 34). We submit that Stimson's activation method as taught is not obvious to our linking process nor reveal our claim element of account identifier. To show obviousness, the examiner has to show that Stimson's teaching would necessarily show the need for account identifier in a database in lieu of using the security code on the cards as seen by one skilled in the art. The question is whether Stimson address our problem of enabling fund transfer between users ? We respectfully submit that Stimson did not.

As for the step "If there is no account identifier associated with said code then prompt user to enter a unique user account identifier, password, storage period and currency to be stored;" we can see there is nothing in Stimson that allows the user to create his own account identifier at the database. All authorized prepaid cards according to Stimson comes with a security number whereby in substitute can be user account number or a PIN known to user stored in the card itself. (Col 6 line 29 to 34). In short, these PIN is stored on the card (not database) and is checked in authorizing payment transaction.

Our claimed 14 assumes that the card is already activated at point of sell, that is both the exact code on the card and the exact code in the database are found. But we are claiming the linking process which goes further by having the user to create his own account identifier of his own choosing so the prepaid card need not be used further. In short, after the linking process is completed the combination of password and user identifier entered will replace the security code under the linking step. This is not obvious in Stimson. In all instances, Stimson requires the card's data (security code) as the key to the system. This linking process also includes the elements of storage period, currency and password all are not found in Stimson's database.

As for step "Determining said user account identifier and password for uniqueness against other stored user account identifiers and passwords ", this step is not obvious since this step must necessarily follow on the previous step which was also not obvious in Stimson.

As for step "Calculating the stored value; Output stored value to user; " both are not obvious since they follow all the previous steps not found in Stimson. As we mentioned the stored value may be different from that in the original card at activation depending on the currency and storage period. Since Stimson stores the exact value on activation (Col 5 line 67) there is no calculating stored value and output calculated value.

Our step here means the activation or original amount initially stored in the local currency can be stored in accordance to the required period and currency by consent. This step which links the last two elements are also not found in Stimson.

As mentioned, the amount to be purchased in Stimson is determined by the user (Col 5 line 67) and not as calculated by the system using variables such as storage period or currency as per our claim. While it is well known in the art that prepaid services card comes with a pre-determined period of usage, this factor however is set at the factory and not by user as per our limitation. Similarly, the examiner mentioned in Final Action that it would be obvious to have different currencies to be stored given the internationalism of trade. The applicant submits that it is not well known to do so in a system that links the amount to an account identifier, the subject matter as a whole which is not obvious. Neither is it obvious for user to set their own period of storage contrary to existing art. Even if it is possible to do so, this implicitly means the manufacturer recognized this need but by itself is not taught in Stimson.

Furthermore, Stimson taught using the prepaid card as the only means to make payment after activation and this would not be obvious to our need to use account identifier once the floating amount is stored. (See our specification Page 10, lines 1-5). Once the amount is stored or linked to account identifier, the pre-paid card in our claimed invention is no longer used unlike Stimson's teaching of using prepaid card for all purposes after activation. In fact the card is the key with the PIN stored within. To discard the card would mean actually losing the money stored in database.

While Rosen taught of user to user account identifiers stored in money modules, there is no teaching of user able to link stored funds in prepaid cards to the modules or how this could be achieved. Rosen only teach of electronic money representation having claims from deposits or credit stored in the module. No calculation of stored value is known in all three prior arts which the examiner admitted at page 7 for claims 26-28 by

referencing the stored value formula. In short if no formula can be found in all the prior arts, then it is equal to admitting no step in calculating the stored value in Claim 14,18, 23 since the calculating step requires the formula. The merit of the formulation will be discussed later.

The motivation/ reasons factors for combining.

The examiner cited that "....in order to provide a stronger protection element to the debit/stored value card system: the card user will be assured that only once properly activated by him/herself, will the account associated with the card be accessible for transactions. "

This citation confuses the subject matter at hand being one linking to an account identifier and one of activating a card as in Stimson. There is no evidence in Stimson to show using an account identifier. For the record an account with a security code for activating a prepaid card as in Stimson is not the same as creating an account identifier and storing the funds for X period and in Y currency both which are not taught by Stimson. Stimson taught of activating the card for purchases while we are teaching of removing the authority from the prepaid card by substituting access by way of an account identifier which is not obvious. In Stimson only when the card is exchange for money can it be activated for used which basically means flagging the security code in the account for use. In contrast, we are claiming to create an account identifier separately in lieu to the security code account as an alias.

Therefore, activation is not an issue but creating/linking account identifiers is and how money is eventually stored is, which is the difference as a whole not appreciated by the examiner's analysis. Furthermore given Stimson already stored funds in the database (albeit not activated), what possible reasons could there be to recalculate the stored amount again upon activation ?

For a 103(a) rejection, the suggestion must be found in the prior art. See Kolmes v. World Fibers Corp., 107 F.3d 1534, 1541, 41 USPQ2d 1829, 1833 (Fed. Cir. 1997) (Invention was not obvious where there was no suggestion or motivation to modify teaching of reference.)

The examiner also did not suggest any evidence from David nor Rosen to combine in view to show obviousness despite stating that it would be obvious to do so in a system based on David, Stimson and Rosen. (Page 7 of current CPA action letter) citing only that it provides stronger protection and with the account associated with the card be accessible for transaction.

While stronger protection may be a motivating factor in general in line with most payment system, it has to be suggested by Stimson by first recognizing the security weakness in the card. If this problem was not first identify in Stimson how would one skilled in the art read the need for stronger protection ?

To rely on stronger as the motivator to one skilled in the art, the examiner would need to show that our method is well known as the desirable 'stronger' alternative based on account identifier linked to pre-stored value in a database or it is well known in the art that modules using claimable deposit is stronger as compared to pre-paid cards in Stimson. Neither was articulated which is not the standard to show obviousness.

In fact, random generated numbers or codes as in Stimson's prepaid cards would prove more difficult to crack then a mere password cum user identifier of user's choosing. This is because humans have limited capacity to remember beyond 6 digits and hence incline to associate birthdates, dictionary words or minor mis-spelling as passwords or identifiers which are more easily crack then random numbers. In fact by substituting the card for a linked account identifier would be less secure. Therefore it is difficult to

understand how would one skilled in the art would find it desirable to adapt a lower standard while being motivated by the need for higher security as suggested by the examiner.

David's provisional application actually states it is an alternative to encryption and presumably is stronger on its own merit (at page 2 of provisional). However, David in CIP teaches uses encryption at para 56 which we submitted is new subject matter. Rosen actually uses a proxy account identifier which may be "serial number " and is never changed (Col 12 line 33) embodied in the money module and not as per our claim in the server created by user of own choosing. However, Rosen also use digital certificates and encryption in modules on presentation. Surely these are more secure than using account identifier cum passwords.

Therefore, our conclusion is that impermissible hindsight was used and we submit that the claims 14, 18, 23 are patentable over Stimson in view of David and Rosen.

Claims 26-28

We respectfully transverse this rejection.

Claim 26 is dependent on Claim 14 while Claims 27 and 28 are dependent on 26 and the difference only being the class. Therefore, we will use Claim 26 as the representative here. As we mentioned Claim 26 is dependent on 14 and hence incorporates all its limitation which we have submitted to be patentable. Claim 14 is dependent on Claim 13.

Claim 26 details calculation of stored value.

Referring now to Claim 26's on its own merit, the examiner asserted using personal knowledge that it is well known in the art that fees and/or cost for services vary on many factors etc.

For convenience, we have restated in quotation "However it is well known in the art that fees and/or costs for financial services rendered by institutions to clients vary from institution to institution and also from client to client within each institution, depending on many factors, including the size of the institution, its business goals, the desirability and loyalty of the client to the institution, etc. A conversion rate would follow the same principles and would inherently be different from institution to another, and maybe for one client versus another within an institution. Therefore it would have been obvious to one ordinarily skilled in the art to use a conversion formula structured as recited in these claims in order to reward clients for loyalty, amount of past business, and other positive factors and provide them incentives for continued patronage of each such institution."

We respectfully disagree since the examiner not only did not provide any evidence and stop in identifying these factors or alternatively how these factors assumed our formulation method. While these individual elements are old in the art, it may not be well known to express it as taught by our specification for storing funds linked to an account identifier (reading the claim as a whole which details a formula including multiplication factor and not merely the elements in the formula) as reiterated in part below.

Stored value = B * D* L * C* R

Furthermore, this fee is embedded in the formula as a stored value and not merely a direct charge as asserted by the examiner common in the art.

The examiner continued by stating that " A conversion rate would follow the same principles " which is again from a personal knowledge stance rather than from one ordinary skilled in the art since no judicial notice is given. There is no evidence to show that it would follow the same principles and therefore we have to call for evidence under 37 CFR 1.104(d)(2) to show this same proposition. See also Zurko, 258 F.3d at 1386, 59 USPQ2d at 1697 ("[T]he Board [or examiner] must point to some concrete evidence in the record in support of these findings" to satisfy the substantial evidence test). If the examiner is relying on personal knowledge to support the finding of what is known in the art, the examiner must provide an affidavit or declaration setting forth specific factual statements and explanation to support the finding.

The issue here is not simply because institution practices some form of fee calculation based on certain parameters as suggested by the examiner and said "would follow" a conversion rate hence render our claim elements to be obvious. Why should it when the one is for fee determination while our claim is for storage of funds ? If not then it is clear that the examiner has defined the problem in terms of its solution. In short, the examiner saw the solution to be 'similar' by identifying the elements and made that as a basis to find similar process and to conclude that it follow the principle. Orthopedic Equip. Co. v. United States, 702 F.2d 1005, 1012, 217 USPQ 193, 199 (Fed. Cir. 1983) ("It is wrong to use the patent in suit as a guide through the maze of prior art references, combining the right references in the right way so as to achieve [a desired result].").

Furthermore, this " would follow " qualification is not the proper standard of obviousness as it implies some possibilities which might or might not follow to our claim. There is no scientific fact or business rule to show this qualification or authority. The test of obviousness is not one of probability or possibilities but one of evidence and facts to prevent falling into the trap of hindsight. The standard of review applied to findings of fact is the "substantial evidence" standard under the Administrative Procedure Act (APA). See In re Gartside, 203 F.3d 1305, 1315, 53 USPQ2d 1769, 1775 (Fed. Cir. 2000).

Our formulation is targeted for calculating stored amount value storage for prepaid cards being linked to an account identifier to enable a user to user fund transfer without interacting with payee. Although fees is well known in finance art, it is not well known for a conversion rate that stores funds from a prepaid card linked to an account identifier in view of the claim as a whole.

As noted by the court in In re Ahlert, 424 F.2d 1088, 1091, 165 USPQ 418, 420 (CCPA 1970), the notice of facts beyond the record which may be taken by the examiner must be "capable of such instant and unquestionable demonstration as to defy dispute" (citing In re Knapp Monarch Co., 296 F.2d 230, 132 USPQ 6 (CCPA 1961)). In short, one skilled in the art must be able to identify the characterization of the formula described in our specification instantly as obvious from knowing fee structure in a financial institution which we beg is not the case here because storing of funds with an embedded fee structured is not known.

Moving to the next issue of motivation or teaching required for an obviousness rejection. None was articulated in particular why would the skilled artisan in the financial services fee with knowledge of a fee formulation, would be motivated to provide a conversion rate to store funds ? This factual question of motivation is material to patentability, and could not be resolved on subjective belief and unknown authority. It is improper, in determining whether a person of ordinary skill would have been led to this, simply to "[use] that which the inventor taught against its teacher." W.L. Gore v. Garlock, Inc., 721 F.2d 1540, 1553, 220 USPQ 303, 312-13 (Fed. Cir. 1983).

In conclusion "conversion rate" as described in our claimed invention within the context of linking said "converted amount" to a user identifier enabling user to user fund transfer originating from a prepaid card as per claim 14 and 13, is unknown in the art, viewing the claim as a whole would not be obvious.

Based on the two legs of our rejection 1) unsupported personal assertion and 2) lack of evidence of teachings or demonstrable motivation, we respectfully call the examiner to allow claim 26-28.

Claims 29-31

We respectfully transverse this rejection.

The claims here recited the "prepaid or stored value" elements which as asserted by the examiner to be shown in Stimson. We submit that this claim is dependent on Claim 13 and therefore would not have been obvious in view of the arts. Taking Claim 29 as the representative for 30 and 31, we would like to draw the examiner to the main differences between Stimson's teaching of pre paid amount and our stored amount as shown below nothing that our prepaid and stored value are not exactly the same.

The two Tables below shows the differences between Stimson and our Claim as seen in a database table format.

Table A showing Stimson

Card _Id	Security Code	Prepaid Value	Top Up	Status
10	1212312145121313	10	0	Not Active
11	1212315421321356	100	2	Active

Table B shows our Claimed Invention

Card_id	Security Code	Prepaid Value	Stored Value	Identifier	Pwd	Status
1	1214521345461	50	NA	NA	NA	Active
2	NA	0	47.25	Hotdog123	XXXX	1 yrs
3	NA	0	18000 YEN	MrBigMan	XXXX	3 yrs

Table A shows what is stored in a database to reflect Stimson's definition of prepaid/pre-stored funds. Card ID 10 shows a card amount that is not activated while Card_ID 11 shows one that is as taught by Stimson. By activation, Stimson merely suggests the card has been sold and the amount can be used for purchase now. The Column Top Up shows how many times a card has been top up or added value.

In contrast as shown in Table B, our version of prepaid/stored value is different to Stimson's. Given this Claim is dependent on Claim 13, it means it is for user to user transfer with characteristics as found in Card_Id 2, 3 of Table B. As we can clearly see our prepaid means no more security code and has additional features and stored value given its usage is 1 yr for Card_ id 2. This 1 yr is set by the user and not the manufacturer or service provider. In Card_ID 3, the user has chosen Japanese Yen which is converted using our formula. In Card_ID 1, it shows a card where its prepaid value is 'floating' and the security code is needed to use the card as per Stimson. In contrast with Stimson, once a prepaid amount is stored, the prepaid has no value signify the important difference between prepaid and stored in our claim

here. Note data above is only for illustration and we assume the original prepaid value for Card_id 2 is USD 50 before storing and Card_id 3 to be USD 200 (both are not shown).

As seen above, we submit implicitly that the said unstated differences were not appreciated by the examiner because no evidence was presented inherently or explicitly to reason the differences on record. This is the third Graham factor: the difference between the prior art and the claims at issue, as viewed from the vantage point of one of ordinary skill in the art must be considered first and failure to do so would implicitly mean the graham factors were not applied consistently. A claimed invention is unpatentable as obvious "if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." 35 U.S.C. § 103(a) (1994); see Dembiczak, 175 F.3d at 998, 50 USPQ2d at 1616.

Given that there are clear evidence above supporting the differences between our version of prepaid or stored value to Stimson's prepaid version, said difference would not be obvious given no teaching in Stimson or in view of Rosen or David to combine each other features. As we said Stimson did not even identify our need hence solution for user to user transfer.

In particular, Rosen did not teach a system under payer's control and without payee interaction. Even if we can accept this suggestion, the structure and design of Rosen is such that there still is some form of interaction between the respective payer /payee modules. No explanation was provided as to how modules can be integrated into David's ISP based system or why would should Rosen apply pre-paid funds in lieu of electronic money from claimable deposits to reach our claim. As it is well known, deposit claims are actually funds belonging to the user (not bank) while prepaid has the meaning where funds paid to the service provider as in Stimson and hence not refundable. Both are irreconcilable and reflect different accounting solutions applying to different subject matter, ie David for credit cards, Stimson for debit/prepaid cards and Rosen for credit lines and deposits.

Motivation.

The examiner provided the exact same reasoning for motivation as per Claim 13 even though this Claim actually refers to pre-stored or prepaid funds found in a user to user system. See, e.g., McGinley v. Franklin Sports, Inc., 262 F.3d 1339, 1351-52, 60 USPQ2d 1001, 1008 (Fed. Cir. 2001) ("the central question is whether there is reason to combine [the] references," a question of fact drawing on the Graham factors).

The motivation here repeats the need for secure, convenience and desirability for the 3 type of cards even though Claim 13 and this Claim has no reference to cards and fail to reflect the differences looking at the claim as a whole. This claim refers to funds stored in a database. Each of the motivating factors have already been discussed above at claim 13 and summarized below:

If by combining the 3 prior arts could only mean installing all the 3 designs in a black box with each operating on its own then the examiner failed to show how each combinable elements could work together and the suggestion to combine is one tainted with impermissible hindsight. The examiner's duty is to show the specific understanding or principle within the knowledge of a skilled artisan that would motivate one to apply a user to user fund transfer system as in Rosen with Stimson's pre-stored cards or David's credit cards and not only to show the generality of said combination since individually each of the teachings do provide a secure, convenient and highly desirable system using their own respective cards/modules

Neither of the 3 prior arts suggested any deficiency in security or convenience or desirability on its own and in particular, Rosen's distributed modular system and the only one that shows user to user transfer using account identifiers made no suggestion to use prepaid cards nor a suggestion to substitute modules to one of a server hosted database to effect transfer. There is no suggestion in the 3 prior arts for an universal system using all the cited payment instrument ie "for users of credit, debit and prepaid cards on a global" (Note the examiner did not include Rosen's claims on deposit and Rosen did not teach of using prepaid card, prestored card). As stated in Fromson V Advance Offset Plate Inc, 755 F.2d 1549, 1556, 225 USPQ 26, 31 (Fed Cir 1985) (the prior art must suggest to one of ordinary skill in the art the desirability of the claimed combination) . In short since the three prior arts are secure, convenient and desirable would combining them result in more of said features and if not how do these features motivate ?

As for security, we have already previously submitted there is no evidence that our system of using identifiers and password would be more secure than a prepaid card using random numbers as access to reveal our method. In fact on the contrary, the examiner actually supported the use of prepaid cards which actually fails to reach this Claim of using account identifiers for user to user fund transfer wherein the funds are stored in a database. (Reading Claim 13 with this claim 29) No evidence to combine with Rosen's modules feature was shown by the examiner even though a single module would effectively store electronic funds securely as taught by Rosen but is not compatible to the examiner's calling for using cards.

As for convenience, the examiner stated that it is convenient to use all 3 type of cards which also fails to reach our claim since we do not use any cards in Claim 13 or 29. We simply refer to the stored funds as claimed. But if convenience is the motivating issue then it is well known that a single card with access to credit/debit and prepaid facilities would be more convenient that using multiple cards. No evidence to combine with Rosen's modules feature was shown by the examiner even though a single module would appear to be more convenient than having 3 type of cards.

As for desirability, we have already submit that a single card would deem to be more desirable than having multiple cards.

In conclusion, for the examiner to show prima facie obviousness, there is a need to show that the differences between our claim and Stimson's teaching is insignificant to reveal the subject matter of user to user fund transfer using stored funds as obvious. We have submitted that this is significant since there is no teaching of using stored value which is different and dependent on a formula etc as detailed above. The question is why would the skilled artisan be motivated to convert Stimson's prepaid value to a stored value when there is no teaching of the need of user to user transfer using account identifiers. As we stressed Stimson's prepaid card system would not be suitable for fund transfer to another user given the need to expose the security code. A risk no reasonable person would take.

Secondly, the combined features do not actually reach our claimed element one of stored value where we have differentiated above as not the same as prepaid in Stimson. The examiner had stated "It would have been obvious to one ordinarily skilled in the art at the time the invention was made to combine the features and capabilities taught by David, Stimson, and Rosen to provide a secure, convenient, and highly desirable electronic transaction system for users of credit, debit, and prepaid cards on a global, worldwide basis." While we teach of using a prepaid card, it is also one capable of being converted to stored value by linking to an identifier unlike Stimson which is basically a general prepaid card. The only novelty in Stimson is able to add value but this is not the same as stored value which includes period, currency and desirability of user etc (elements found in the formula).

Therefore, we must respectfully ask claims 29-31 to be allowed based on the reasoning above and in view of what is known in the art, the examiner had failed to consider the significant difference between Stimson's prepaid and our stored value or alternatively implied there is no difference as viewed by the

skilled artisan, the combined features of applying 3 type of cards actually fall short to meet our stored value element as taught in our specification and lack of identifiable teachings to combine the features to show the claim as a whole.

Claims 15, 19, 24.

This rejection is respectfully traversed. We have grouped all claims 15,19,24 as they have the same elements except for different classes where Claim 15 is the representative.

The examiner stated David: Abstract; Summary of the Invention: Page 2, P22; P7, P85-88: Fig 6-8, associated text; and Stimson: C2, L1-4; L25-30; L32-36; L38-39; L42-44; C3 L64-67; and Rosen: Abstract; Summary of the Invention; Fig 36 and 46, associated text) as evidence to show obviousness.

We would like to note here for the record that Claim 15,19,24 were previously rejected in Final Rejection using only one single prior art ie David under 102(e). Subsequently in our CPA, with only one amendment by adding the word instantly, this is now being rejected under 103(a) by 3 prior arts as stated above.

A claimed invention is unpatentable as obvious "if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." 35 U.S.C. § 103(a) (1994); see Dembiczak, 175 F.3d at 998, 50 USPQ2d at 1616. "The ultimate determination . . . whether an invention is or is not obvious is a legal conclusion based on underlying factual inquiries including: (1) the scope and content of the prior art; (2) the level of ordinary skill in the prior art; (3) the differences between the claimed invention and the prior art; and (4) objective evidence of nonobviousness." Dembiczak, 175 F.3d at 998, 50 USPQ2d at 1616 (citing Graham, 383 U.S. at 17-18, 148 USPQ at 467). Further "that the best defense against the subtle but powerful attraction of a hindsight-based obviousness analysis is rigorous application of the requirement for a showing of the teaching or motivation to combine prior art references." Id. at 999, 50 USPQ2d at 1617. That suggestion may come from, inter alia, the teachings of the references themselves and, in some cases, from the nature of the problem to be solved. See Pro-Mold & Tool Co. v. Great Lakes Plastics, Inc., 75 F.3d 1568, 1573, 37 USPQ2d 1626, 1630 (Fed. Cir. 1996); Rouffet, 149 F.3d at 1355, 47 USPQ2d at 1456.

As an initial matter, we disagree with the examiner that substantial evidence supports the finding that David, Stimson and Rosen contain all the limitations set forth in claim 15 which is the representative here.

Starting from the preamble itself, "convertible prepaid card" and in "any currencies" are not disclosed by David (See Appendix 2). While David's provisional shows credit card and payment amount, we submit that these two elements would not "necessarily" show a convertible prepaid card capable of paying in any currencies as disclosed in this claim. However, Stimson shows a prepaid card but not a convertible one to any currencies as asserted by the examiner or from floating (prepaid) to stored value. In fact a word search for 'convert' is not found in the entire Stimson's patent disclosure. Rosen shows any currencies are asserted by the examiner but on closer reading Rosen actually taught of foreign currency exchange between two users. While this means in any currency, the reasons for doing so are different where our claim refers to paying a merchant including a merchant server, Rosen taught user to user foreign exchange method at Fig 46 of Rosen. We submit that a foreign exchange method would not be obvious to one skilled in the art to reveal prepaid convertible cards since the said foreign exchange method uses money modules.

Referring to the body of the claim, we submit that the steps below are not meet by David

"generating a first dynamic transaction code to the host server"

"generating a second dynamic transaction code to the purchaser"

"requesting purchaser to provide second transaction code and security code from prepaid card" (Note examiner wrote payment card instead of prepaid card in page 5 of action letter which is not correct)

"receiving the second transaction code and security code as inputted by purchaser; "

"authenticating the first transaction code and second transaction code; "(Assuming vendor's request is inherent to first transaction code but there is still no second transaction code)

" authenticating the said security code for validity; " (David oppose sending security codes over unsecured lines)

In David's the vendor's server actually send a single purchase authorization request containing information about the merchandise to be purchased, identifying information about the proposed purchaser, some of which is the identifying information assigned by the ISP about the subscriber/purchaser to the ISP (Page 5 of Provisional). This does not inherently or explicitly shows our dynamic code which is generated to provide 'half' the purchase request. David teach issuing a single complete source request for the transaction and not as in our claimed invention where the code issued to the host server forms only part of the request. The novelty here is in splitting the transaction codes into 2 which is not taught nor obvious.

Even if David suggested creating a code to the host server, David certainly did not teach sending the second transaction code (the other 'half') to the buyer or where the said code is inputted to the host server by purchaser (in step " requesting purchaser to provide second transaction code and security code from prepaid card ") to complete the authentication using the check sum method as per our specification.

In fact the invention in David as taught in the provisional application relies on IP address and Buyer-ID code in order to identify.

At the host server, this is followed by requesting the second transaction code and security code from the prepaid card which is not found in David. Even if we substituted a prepaid card to a credit card as in David, the fact that transmitting static numbers over the Internet is expressly opposed by David. As mentioned, David distinctively argues that sensitive information should not be sent on an unsecured line. (See pg 4 where David's disclosed about sending credit card information by conventional means).

We managed to solve this problem by having one static sets of code (security code) combined with a dynamic code (transaction) to be send at the same time which makes it harder for hackers then if only the static number is sent alone or chaffing them. This step of combining both static and dynamic codes ('second code') would not be obvious since there is no second code in David and David expressly taught away from sending card numbers.

Similarly because there is no second code forming the other half of the purchase request in David, it would not be obvious to authenticate the first transaction code and second transaction code as taught in our specification. Our authentication method includes first combining both codes to form the base code satisfying that the purchase has actually confirmed the order and the order indeed originates from the merchant. For example the base code could be Z from both codes X and Y hence Z=X+Y (as an example) where X is send to the host and Y is send to the purchaser and Z is a value known to the host to identify the merchant. There is no teaching in David to show such authentication method.

As David uses debit cards (citation P 85-88 in CIP) are only found in the later CIP hence not qualifying for the earlier filing date as at July 30, 1999, David's system would not be able to instantly crediting the amount requested for payment to merchant account.

The steps of instantly debiting and crediting or double book entry is also not found in David. As mentioned this is a significant step found only for prepaid cards rather than in debit or credit cards since debit facility requires the issuing financial institutions to settle the transactions and credit card is only billed periodically in order to capture the interest expenses or borrowing cost. In short if payment is instantaneous, then credit card would not be credit instrument at all since credit refers to cost of money over a time period.

Even if the credit card may be substitute in view of Stimson's prepaid card, there must be motivation to combine readily found in the prior arts as seen by one skilled in the art. This would be difficult since David did not suggest using a prepaid card and Stimson's teaching of prepaid cards or any cards in the future is only related to the Stimson system and not as one described by David. As David stated, the cards must be presented to the ISP first before being used for purchases which is different to Stimson's teaching of activating the card using a terminal.

It is also well known in the art of banking that a credit card is more desirable to a prepaid card in terms of convenience hence the higher fees involved as there is no requirement to constantly reload/recharge the cards. There is no further evidence to show David's security is any less than as described in Stimson to motivate one skilled in the art to combine with a prepaid card.

<u>The motivation factor.</u>

The examiner provided the reasons as " to provide a secure, convenient and highly desirable electronic transaction system for users of credit, debit and prepaid cards, worldwide basis. " Since this is the same reason as previously submitted in Claim 13, we incorporate by reference our previous submitted rebuttal found in Claim 13 whereby the pertinent points are mentioned below.

We submit such motivation implicitly suggest that any one single system is not as secure, convenient and highly desirable unless combined together to accommodate the various payment cards. We find such motivation flawed as it does not appears to be suggested by the prior arts. The examiner did not pointed to any suggestion from the prior arts to show that by combining each of the payment cards system it would necessary provide "secure, convenient and desirable" as reasoned. This further assumes that one skilled in the art is desirous of using credit, debit and prepaid cards in a single universal system and the presented prior arts suggested so; which is not the case. "[w]hen determining the patentability of a claimed invention which combines two known elements, 'the question is whether there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination.'" In re Beattie, 974 F.2d 1309, 1311-12, 24 USPQ2d 1040, 1042 (Fed. Cir. 1992) (quoting Lindemann, 730 F.2d at 1462, 221 USPQ at 488).

We also further submit that because of the different nature between credit, debit, prepaid cards and electronic money/notes in different currencies drawn from deposits, one skilled in the art will not be tempted to combine in view of David's, Stimson's and Rosen's teaching resulting in an inoperable device. It is well known in the art that a debit card could not be used directly in a credit card system or vice-versa because of its billing, accounting and business processes are not compatible. A credit card uses credit line extended by an institution while a debit card applies the holder's own funds. Similarly when one skilled in the art looks at Rosen using E-M would not find it desirable to combine with card payment system. There

must exist in the view of one skilled in the art whereby said money modules system as promoted in Rosen is less desirable to a card payment system in order to combine.

While it may be convenient for ordinary users to have as many payment devices as a consumer choice, such view is not one of the skilled artisan who will have to integrate the 3 systems. It is well known in the art of IT integration that it is never convenient to integrate 3 different systems. In fact the task is impossible given the 3 incompatible accounting and billing backend.

Even if we view from ordinary user, convenience may not be suitable as a motivator given not every user possess a credit card (this depends on user's credit rating) or a module or debit card issued by a bank (this will depend on the bank offering this service and the type of account) . However, most users would have access to a prepaid card which is basically a purchase transaction. Therefore to suggest combining all the 3 systems features for convenience sake seems to ignore the fact that not all users have access to these cards. And it also does not reach our claimed invention as we did not seek credit/debit card or deposits from banks. As we mentioned previously the trend now is to use a single card not multiple cards.

The examiner also failed to point out distinctively how and which features from the prior arts could be combined to meet the method claimed in particular why would it be obvious to have 2 separate half of codes for the same purchase request. Ex parte Re Qua, 56 USPQ 279 (CCPA 1942) at 280. The claimed invention must be considered as a whole, and the question is whether there is something in the prior arts to suggest the desirability of using a server merchant to issue two half sources of transaction codes. In short, if David's teaching of using a single response from merchant server is adequate why do we need two halves of the same code ?

David only reveals using passwords to confirm transaction in provisional (Fig 3,4,5) or as in the later CIP (Fig 6,7,8) showing Toolbox and finger print file see (Para 0144). Both are not codes issued by the vendor server as our claimed invention. As we mentioned Fig 6,7,8 are not found in provisional and hence constituted new matter.

We respectfully ask the examiner to transverse this rejection as not all elements are found explicitly or inherently and the provided motivation by the examiner is not found in all three prior arts to show our claimed invention as a whole in particularly why the element of a second half transaction code is not even found. It is also questionable whether the combined features from the 3 prior arts do provides better security as versus adequate security individually or why do we need 3 different type of cards to reach our claim for prepaid only.

Similarly we respectfully submit that Claims 19 and 24 be allowed based on the reasoning as in Claim 15 as the only differences here is the class type of claims.

Claims 16, 20, 25

This rejection is respectfully traversed. We have grouped all claims 16,20,25 as they have the same elements except for different classes where Claim 16 is the representative.

The examiner stated Rosen: Fig 36 and 46, associated text) as evidence to show obviousness.

As an initial matter, we disagree with the examiner that substantial evidence supports the finding that Rosen contain all the limitations set forth in claim 16 which is the representative here.

While Rosen shows both user to user fund transfer and foreign exchange, they are taught within the context of two parties changing one currency for another hence establishing the rate of exchange. In contrast, our claimed is for a payment to a merchant using a prepaid card where if the said card's currency is not the same as required for payment to the merchant. Say the card is in US dollars and the merchant requires payment in Yen. In Rosen, the user has to initiate their respective money modules not prepaid cards or stored value in the database and its not initiated due to a different currency payment.

In particular this claim is only trigger when the payment amount requested is in a currency other than the prepaid card's currency and the steps are taken by the host server and not by the users. (See preamble "... where the said amount payable is in a currency other than prepaid card's currency...")

In short, our claimed steps are in response to the amount payable being in different currency and the steps are at the host server (the structural limitation). In Rosen, it taught user wanting/willing/desiring to exchange currency with another user (Fig 46) using money modules. Given that Rosen did not teach a host server requesting purchaser to convert where the amount is in a different currency, the first step of requesting purchaser to convert the equivalent amount in prepaid card's currency to the requested foreign currency amount if the balance in the database is more than the requested equivalent foreign currency amount for payment " is not met.

Further noting that this step also need to check if the converted amount equivalent is greater than balance in database before a request can be issued by host server. In short, this step incorporates two distinct steps first which is to detect if the currency is foreign to the prepaid card and secondly only when the converted amount satisfied the requested payment amount.

In Rosen, the steps as shown in Fig 46 shows two users establishing the exchange rate while in our claim step, the host server is requesting purchaser to convert further implying that the exchange rate is already established and this request is triggered by the presence of amount payable in foreign currency and not two users wishing to exchange currencies.

As this is a request by host server, this would not meet the requirement for two users in Rosen. And once purchaser has agreed the converted amount is credited for merchant account instantly. As one can see there is no interaction with merchant on the rate as shown in Rosen (assuming the merchant inherently shows second user).

In summary, we submit that Rosen could not have meet all the limitations because Fig 46 is primarily designed for Subscriber to Subscriber Foreign Exchange as titled in Fig 46. The teaching taught of interacting with the two subscribers while we claimed purchaser being requested by Host Server. The amount payable is for paying a merchant presumably for a service or product priced in a foreign currency. There is no merchant account as in Rosen's Fig 46 and even if it inherently shows Subscriber B to be a merchant it still could not also inherently shows the merchant to be a host server since our purchaser interact with the host server and not any merchant or subscriber. This is an important structural differences between Rosen's modules concept and our host server.

Turning to the examiner's cited motivation " It would have been obvious to one ordinarily skilled in the art to have included the capability for a payer to approve currency conversion rates prior to agreeing to a transaction, so as to make sure that no dispute would later arise as to the fairness of such conversion operations. " at page 6.

It appears that the above motivation is from the examiner's personal knowledge and therefore judicial notice must be taken. The examiner shows no evidence for this assertion and therefore the applicant respectfully request for such under in 37 CFR 1.104(d)(2). We further submit the prevailing art does not

support so in particular in Stimson where a prepaid card was taught to be used for purchases but made no mentioned whether our claimed steps will be initiated when it detects a different currency.

As we mentioned Rosen only teach user to user doing foreign currency exchange and hence it is appropriate for the two parties to negotiate a rate acceptable between them since they are exchanging money with money and not as in our claimed for payment of goods. David obviously does not have this step as it is well known in the art for credit cards to be billed later at the rate determined by the credit card company or bank if the amount payable is in a foreign currency. Given this widely accepted practice of not allowing user to confirm or reject and with no noticeable complaints by credit card members, how would it be obvious to show 'fairness' as the motivator now for prepaid cards as suggested by the examiner ? Stated differently, we could but conclude the impermissible hindsight was used.

Furthermore, a 103 (a) rejection for obviousness must consider the subject matter of the claim as a whole which in this case is the triggering mechanism on detecting the amount payable in foreign currency. There is nothing in Rosen to teach this 'trigger' and as mentioned Rosen taught of two willing buyer and seller of currencies and not as our claimed subject matter of converting the local card currency to another upon detecting this requirement on payment presentation. This would be a clear indication that the most pertinent prior art (Rosen) is not within the scope nor is considering the same problem as the applicant which is the desirability for a prepaid card system capable of converting payable foreign amount on request for purchases (taking the claimed as a whole).

Therefore even if it is obvious for one skilled in the art to consider the fairness as a motivating factor in general, such suggestion is not found in all the prior arts evidence hindsight by the examiner.

Claim 21

This rejection is respectfully traversed. This claim refers to the elements found in the transaction code.

The examiner stated David discloses all the limitations of Claim 21 (P 5 and P56) and Stimson in particular specifically discloses " predetermined time period " for use of debit cards in his system (Col 2, lines 16-24)

As an initial matter, we disagree with the examiner that substantial evidence supports the finding that David contain all the limitations set forth in claim 21. In particular P 5 describes the general state of using encryption as a way to transmit data across as at filing date 30 July 1999 and P 56 refers to teaching of using encryption for David's invention which constitute new matters as we pointed out earlier and which has been confirmed by testing with plagiarism software as detailed in Appendix 2. One must be absolutely clear between what is noted as the general state of the art as in P5 and what is described as part of David Invention in P56. Encryption is well known even before 1999. In fact, careful reading would reveal that David intended to use a system without encryption by eliminating this step using stored credit card details at ISP (page 4,5 of provisional) but perhaps later changed his mind to incorporate encryption as in the later filed application under P 56. Why David made this reversal is unknown but as P56 did not form part of his initial teaching it does not deserve the earlier filing date.

We have no objection that encryption is well known in the art whether taught by David or by others earlier. However, David on its own still would not have meet all the elements in particular transaction codes, encryption and expectancy. As mentioned, our transaction codes are issued by merchant server and are send to both purchaser and host server consisting of 2 different halves which is distinct to David's purchase

order request which is only send to the ISP. As the transactions code in Claim 21 is dependent on Claim 19's limitation, this means it is similarly a separate half of the complete code.

Turning to expectancy, the examiner asserted that Stimson shows the cards having this feature and concluded that this meets our limitation. We beg to disagree . While Stimson taught of this feature, this is only for security codes on prepaid cards and not necessarily as the dynamic transaction codes as transmitted by the merchant server to purchaser and host server which are not taught. The examiner provided no explanation as to how a feature taught to be for prepaid cards could now also be used for codes transmitted by a merchant server such that it would be obvious for one skilled in the art to combine this feature in view of Stimson.

As noted in Stimson, the merchant server does not transmit any codes and Stimson's codes here refers to pre-paid card security codes rather than generated dynamically by merchant server. (Col 7 line 1 to line 20.) To meet this expectancy limitation, Stimson must show that said codes are similarly issued by merchant server and dynamic. Further, codes on a prepaid card as in Stimson are static and how it would be obvious to show expectancy and dynamism has yet to be explained by the examiener.

Even if all the elements are meet, there still must be motivation to combine to reach our claimed invention. There must be a showing from the prior arts suggesting it is desirable to apply some expectancy to the transmitted codes issued by the merchant server and not inferring such codes as found in prepaid cards is obvious to show the same feature for our dynamic codes, both uses being different. In re Werner Kotzab, 217 F.3d 1365,1371, 55 USPQ2d 1313, 1317 (Fed. Cir. 2000) ("[A] rejection cannot be predicated on the mere identification. . . of individual components of claimed limitations. Rather, particular findings must be made as to the reason the skilled artisan, with no knowledge of the claimed invention, would have selected these components for combination in the manner claimed."). Here, there is no such evidence presented to show that one skilled in the art is aware of our dynamic codes as transmitted by merchant server since this was not taught by any of the prior arts so how could one combining with what is unknown.

Towards the end, it appears that the examiner presented all the elements and did not elaborate further how it would be desirable to combine all these separate elements. As the examiner did not provide any reasons/motivation to show the combination (see page 5 of action letter) as required under a 103(a) rejection, we must submit without prejudice that this claim on its own is patentable. See In re Dance, 160 F.3d 1339, 1343, 48 USPQ2d 1635, 1637 (Fed. Cir. 1998); Gambro Lundia AB, 110 F.3d at 1579, 42 USPQ2d at 1383 ("The absence of such a suggestion to combine is dispositive in an obviousness determination.").

Application number: 09/396005 **Art Unit:** 3621
Applicant: Khai Hee Kwan **Examiner:** David Q. Le
Title: Method, apparatus and program to make payment in any currencies through a communication network system using prepaid cards

Declaration 37 CFR 1.132

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of any application, any patent issuing thereon, or any patent to which this verified statement is directed.

18 Dec 2003

Khai Hee KWAN
P.O.Box 1178
Sandakan 90713
Sabah, Malaysia

Appendix 1

MARKED VERSION

Without conceding the validity of the examiner's argument or the undemonstrated prima facie, and to expedite prosecution of the application, the claims are hereby amended as below and we respectfully seek the examiner's permission to add the following amendments:

13. (Previously Presented) In an Internet system having a plurality of computers connected by a network, a user to user payment method executable at host server having a database to transfer stored funds in any currencies over a network under payer's control, comprising:

prompting payer to input payer's account identifier and password;

authenticating the said payer's account identifier and password for validity;

prompting the payer to input payee's account identifier and fund transfer information;

receiving said payee's account identifier and fund transfer information;

upon authenticating the payee's account identifier, instantly crediting the fund to payee's account if the balance in the database associated with the payer account identifier and password is more than the fund for transfer;

instantly debiting the balance associated with the payer's account identifier and password in the database with the said fund transferred to payee's account; and

whereby said transfer is made without interacting with payee.

14. (Currently Amended) The method of Claim 13 includes a step of storing and linking prepaid card amount to an user account identifier in the host server over a network comprising:

prompting user to enter security code associated with the prepaid card;

receiving the security code;

determining if the security code is valid;

determining if any identifier account is associated with the security code;

if there is no account identifier associated with said code then prompt user to enter an user account identifier, password, storage period and currency to be stored;

receiving the said user account identifier, password, storage period and currency as inputted by user;

determining said user account identifier and password for uniqueness against other stored user account identifiers and passwords;

calculating the stored value;

output stored value to user;

if said user account identifier, password combination is unique and stored value is acceptable to user then add said account identifier and password into database linked with the stored value amount; ~~and~~

if said user account identifier, password combination is not unique and stored value is acceptable to user then linked the stored value amount to said existing user account identifier and password in the database; and

whereby upon completion of storing and linking said prepaid card is valueless.

15. (Currently Amended) In an Internet system having a plurality of computers connected by a network, a method using a convertible prepaid card for payment to a merchant in any currencies over a network comprising:

at the merchant server, receiving a request for payment for good or services by purchaser;

generating a first dynamic transaction code to the host server;

generating a second dynamic transaction code to the purchaser;

at the host server having a database, receiving the first transaction code from merchant server;

requesting purchaser to provide second transaction code and security code from prepaid card;

receiving the second transaction code and security code as inputted by purchaser;

authenticating the first transaction code and second transaction code jointly at said host server;

authenticating the said security code for validity;

upon authentication of the security code, instantly crediting the amount requested for payment to merchant's account if the balance in ~~the~~ said database associated with the security code is more than the requested amount for payment;

instantly debiting the balance associated with the security code in ~~the~~ said database with the said amount paid to merchant's account; ~~and~~

notifying merchant server and purchaser; and

whereby first transaction code and second transaction code are distinct.

16. (Currently Amended) The method of Claim 15 where if ~~the~~ said amount payable is in a currency other than ~~the~~ said prepaid card's currency further comprising steps at the host server:

requesting purchaser to convert the equivalent amount in prepaid card's currency to the requested foreign currency amount if the balance in the database is more than the requested equivalent foreign currency amount for payment;

receiving approval by purchaser for converting the said equivalent amount to the requested foreign currency amount for the transaction;

instantly crediting the converted amount in foreign currency for payment to merchant's account; and;

instantly debiting the said credited amount equivalent in prepaid card's currency associated with the purchaser's prepaid card account in the database.

17. (Previously Amended) User to user payment system for transferring stored funds in any currencies over a network accessible by a plurality of users comprising:

at least a host server with a database further comprising; a computer storage medium for storing executable program code programmed to perform the method of Claim 13.

18. (Previously Amended) User to user payment system for transferring stored funds in any currencies over a network accessible by a plurality of users comprising:

at least a host server with a database further comprising; a computer storage medium for storing executable program code programmed to perform the method of Claim 14.

19. (Currently Amended) An Internet system using a convertible prepaid card for payment to a merchant in any currencies over a network comprising:

at least a merchant server further comprising;

a computer storage medium for storing executable program code; and

means for executing the said program code, wherein the program code further comprises:

code to receive a request for payment for good or services by purchaser;

code to generate a first dynamic transaction code to the host server;

code to generate a second dynamic transaction code to the purchaser; and

a host server having a database further comprising;

a computer storage medium for storing executable program code; and

means for executing the said program code, wherein the program code, further comprises:

code to receive the first transaction code from merchant server;

code to request purchaser to provide second transaction code and security code from prepaid card;

code to receive the second transaction code and security code as inputted by purchaser;

code to authenticate the first transaction code and second transaction code jointly;

code to authenticate the said security code for validity;

code to instantly credit the amount requested for payment to merchant's account if the balance in the database associated with the security code is more than the requested amount for payment;

code to instantly debit the balance associated with the security code in the database with the said amount paid to merchant's account; ~~and~~

code to notify merchant server and purchaser; and

whereby first transaction code and second transaction code are distinct.

20. (Currently Amended) The system of Claim 19 ~~wherein the said amount payable is in a currency other than the prepaid card's currency~~ further comprising:

code to determine if the said amount payable is in a currency other than the prepaid card's currency;

code to request purchaser to convert the equivalent amount in prepaid card's currency to the requested foreign currency amount if the balance in the database is more than the requested equivalent foreign currency amount for payment;

code to receive approval by purchaser for converting the said equivalent amount to the requested foreign currency amount for the transaction;

code to instantly credit the converted amount in foreign currency for payment to merchant's account; and

code to instantly debit the said credited amount equivalent in prepaid card's currency associated with the purchaser's prepaid card account in the database.

21. (Previously Presented) The system of Claim 19 wherein said transaction codes comprising encrypted purchase information, amount, merchant information and a fixed period of expectancy.

22. (Previously Presented) Computer executable software code stored on a computer readable storage medium implementing the method of claim 13

23. (Previously Presented) Computer executable software code stored on a computer readable storage medium implementing the method of claim 14

24. (Previously Presented) Computer executable software code stored on a computer readable storage medium implementing the method of claim 15.

25. (Previously Presented) Computer executable software code stored on a computer readable storage medium implementing the method of Claim 16 .

26. (Previously Presented) The method according to Claim 14, wherein calculation of the stored value is based at least in part on the formula below;

Stored value = B * D* L * C* R

Where B is the face value of the prepaid card, D is a factor related to storage period, L is factor related to the value and loyalty of customer that is based on his/her past purchases of pre-paid cards, C is factor relating to the cost of money and R is a factor concerning flexibility in currency stored.

27. (Previously Presented) User to user payment system for transferring stored funds in any currencies over a network accessible by a plurality of users comprising:

at least a host server with a database further comprising; a computer storage medium for storing executable program code programmed to perform the method of Claim 26.

28. (Previously Presented) Computer executable software code stored on a computer readable storage medium implementing the method of Claim 26.

29. (Previously Presented) The method of Claim 13 whereby said fund is prepaid or stored value.

30. (Previously Presented) User to user payment system for transferring stored funds in any currencies over a network accessible by a plurality of users comprising:

at least a host server with a database further comprising; a computer storage medium for storing executable program code programmed to perform the method of Claim 29.

31. (Previously Presented) Computer executable software code stored on a computer readable storage medium implementing the method of Claim 29.

Appendix 2

Summary : Differences between David's provisional and CIP on subject matters

We have applied two methods as summaries below to compare subject matter allegedly present in David's original provisional application 60/146628 and Continuation in Part (CIP) US 2002/0073046 A1. Method A consist of our manual examination and Method B using a plagiarism software. The detailed results are summaries as Appendix 2A and 2 B herein attached. The table A below summaries the results of both methods against the examiner's assertions.

Examiner Assertion of Commonality as found in CIP	Resultant: When there is a difference between Method A and B, we resolve in favor of Examiner	Method A- Manual examination of examiner's assertion against Provisional	Method B- Using Plagiarism software *
Abstract	No	No	No
P 5	**Yes**	Yes	No
P 7	**Yes**	Yes	Yes
P 10	**Yes**	Yes	Yes
P 11	No	No	No
P 12	**Yes**	No	Yes
P 13	No	No	No
P 14	No	No	No
P 15	No	No	No
P 16	No	No	No
P 17	**Yes**	Yes	Yes
P 18	**Yes**	Yes	Yes
P 19	**Yes**	Yes	Yes
P 20	No	No	No
P 21	No	No	No
P 22	**Yes**	No	Yes
P 23	**Yes**	Yes	Yes
P 24	No	No	No
P 25	**Yes**	Yes	Yes
P 56	No	No	No
P 85	No	No	No
P 86	No	No	No
P 87	No	No	No
P 88	No	No	No
Fig 6	No	No	No
Fig 7	No	No	No
Fig 8	No	No	No

*Software Used: Wcopyfind (Version 2.2) by Lou Bloomfield,
Professor of Physics, University of Virginia, Box 400714, Charlottesville, VA 22904-4714
Source: http://plagiarism.phys.virginia.edu/Wsoftware.html

Application number: 09/396005 **Art Unit:** 3621
Applicant: Khai Hee Kwan **Examiner:** David Q. Le
Title: Method, apparatus and program to make payment in any currencies through a communication network system using prepaid cards

Parameters Used: Shortest Phrase to Match — 6 words. This number is the minimum string length that WCopyfind 2.2 will consider to be a match.
Most Imperfections to Allow —9 This number is the maximum number of non-matches that WCopyfind 2.2 will allow between perfectly matching portions of a phrase. For example, a value of 0 will limit WCopyfind 2.2 to finding only perfect matches.
Shortest Text String to Consider — 100.
Minimum percentage of matching words 50 %
Fewest matches to report- 100
In short, the parameters are maximized to identify plagiarism or as much common subject matter as practicable.

Note: In addition the Plagiarism software also shows the following paragraphs having similar subject matter or words: P 2, P4, P 6, P 7, P 8, P 9, P 28, P 104.

Resultant of our examination plus said plagiarism software shows that only the following paragraphs have found support from David provisional Application.

P5, P 7, P10, P 12, P 17, P 18, P 19, P 22, P 23, P 25.

Italicize words means missing words being used to gap the sentence for results from Method B.

Table A (Line by Line Manual Examination)

Provisional (page reference)	Subject matter in CIP (Underlined means unsupported subject matter)	CIP-Examiner's citation
Most purchases are conducted in the following manner: a purchase selects his merchandise and the vendor requests payment by one of several methods one of which includes payment by providing credit card information. (pg 1)	Most purchases are conducted in the following manner: a purchaser using a browser application on his local client computer connects via his computer's modem to a dial-up ISP and makes connections through the ISP to various Websites, URL. Purchase selects his merchandise and the vendor usually requests payment by one of several methods, one of which includes payment by providing credit card information	P 7
It is thus an objective of the present invention to provide a method for potential on-line buyers of merchandise marketed over the internet to pay for those purchases without exposure to the risk of credit card theft by electronic interception. (pg 3)	Thus, it is an object of the present invention to provide a system and method for implementing secure transactions including but not limited to purchases over a computer net work.	P 10
No mention is found in provisional application.	Debit Cards	P 85-88
Password but only in Fig 3,4 for confirming a transaction. Fig 6 does not exist in provisional application	User, password, User ID, Fig 6	Fig 6, associated text
IP is mentioned. Fig 7 is not found in provisional application	Includes IP of User, Fig 7	Fig 7, associat

Application number: 09/396005 **Art Unit:** 3621
Applicant: Khai Hee Kwan **Examiner:** David Q. Le
Title: Method, apparatus and program to make payment in any currencies through a communication network system using prepaid cards

		ed text
No mention since Fig 8 is not found in provisional application	Includes PC finger print, Fig 8	Fig 8, associated text
According to surveys and other marketing data, there always has been and there still exists a high percentage of the population which is deterred from purchasing merchandise directly over the internet. This large population apparently fears that , despite all the efforts at security and cryptography promised by the vendors, there still exists the probability that their credit account information will be intercepted on-line by a third party computer hacker and used illegally, at great expense and trouble for the card-holder. ... is that the merchant cannot always be certain that just because he has obtained credit card information, that he will actually be paid for the merchandise he ships. *Encryption is mentioned here for the purpose of explaining the current state of the art and not as part of the invention.*	Most of the disclosed systems have the disadvantage that they rely on the transmission of sensitive information over unsecured network routes and lines for each transaction. Although practically speaking, all the systems which rely on encryption are fairly safe, there is still some risk of credit card misappropriation and there is little psychological comfort given to potential users by their knowing that encryption is being used. In addition, the merchant does not know whether the person making the purchase is actually the person whose name is on the credit card.	P 5
Summary of the Invention: It is thus an objective of the present invention to provide a method for potential on-line buyers of merchandise marketed over the Internet to pay for Those purchases without exposure to the risk of credit card theft by electronic interception. It is a further objective of the invention to provide a mechanism for facilitating e-commerce which will increase the confidence of the consuming public in the Safety of such transactions. It is a further objective of the invention to provide a mechanism for facilitating e-commerce which will increase the confidence with which vendors may ship the purchased product or deliver the purchased service without fear of the payment being provided fraudulently. These objectives and others and others not specifically enumerated herein are achieved by the invention disclosed herein which comprises a method for Providing payment to an on-line merchant for services	Page 2 (Objects of the Invention) P10 to P21 [0010] Thus, it is an object of the present invention to provide a system and method for implementing secure transactions including but not limited to purchases over a computer network. [0011] It is another object of the invention to provide a system and method for permitting users of a network to perform transactions such as banking, purchases of merchandise and/or services and other transactions to be made over a computer network. [0012] It is an object of the invention to provide a system and method whereby the user may feel confident that information including but not limited to private personal information such as credit card or other payment information is not at risk of being diverted, misappropriated or stolen and the supplier may be more confident that the user	P 10 P 11 P 12

or goods provided to an on-line buyer. The method relies on the business relationships between the member computers which form the structure of the Internet. Generally speaking, the Internet is a network of computers, remote from one another, linked by a variety of communications lines including telephone lines, cable television lines, Internet service providers (hereinafter "ISPs") satellite link-ups and the like. Internet service providers (hereinafter "ISPs") provide the link to the main backbone of the Internet for small end users. The account for the end user is established in the normal manner usually by providing credit card information to the ISP by conventional means, such as by voice telephony, fax transmission or check. In most ISP-end user relationships, the ISP has been given credit card information and this information is on file with the ISP and available to the ISP's computers. In return for receiving payment, the ISP provides a gateway to the Internet for the end-user's use. The end-user (or subscriber) is provided with software means and identification codes for dialling directly into the ISP's computers. The ISP's computers assign an Internet Protocol (hereinafter "IP") address to the subscriber for use during the particular on-line session in progress. The subscriber's computer transmits messages which are received by the ISP computer and relayed through the IP address and out onto the Internet to the ultimate intended recipient computer. During the entire time the on-line session in progress, the IP address does not change and is thus available as identifying information. By monitoring and occasionally reverifying that the subscriber's computer is still on-line at the assigned IP address, the ISP can confirm that certain activities could be attributed to the subscriber. The present invention takes advantage of the intimate relationship which is recreated Every time an Internet subscriber's computer goes online and signs into his ISP's computer by assigning to the ISP computer the function of clearinghouse and active intermediary between the subscriber's computer and the vendor's computer.	is bona fide. [0013] It is also an object of the present invention to provide a system and method that permits one or more parties to a transaction to have confidence that the other party to the transaction is who he or she purports to be. [0014] It is a still further object of the invention to provide a system and method whereby a "fingerprint" of the computer or other device used by a party to a transaction is used for security purposes. [0015] It is another object of the invention whereby a one time password may be used to provide security for a transaction. [0016] It is an objective of the present invention to provide a system and method for on-line purchasers of merchandise marketed over the Internet to pay for those purchases with minimized exposure to the risk of billing information theft by electronic interception. [0017] It is an objective of the present invention to provide a system and method for on-line purchasers of merchandise marketed over the Internet to pay for those purchases with minimized exposure to the risk of credit card theft by electronic interception. [0018] It is a further objective of the invention to provide a mechanism for facilitating e-commerce which will increase the confidence of the consuming public in the safety of such transactions. [0019] It is still a further objective of the invention to provide a mechanism for facilitating e-commerce which will increase the confidence with which vendors may ship the purchased product or deliver the purchased service without fear of the payment being provided fraudulently. [0020] It is yet a further object of the present invention to provide a site-specific and	P 13 P 14 P 15 P 16 P 17 P 18 P 19

A subscriber computer signs in to the ISP computer the vendor's computer. When the subscriber system and is recognized and assigned an IP address. Identifies merchandise or services at a vendor's website which he wishes to purchase, he sends programming to the website which selects the items and instructs the vendor's computer to generate a purchase authorization request which is sent to the ISP computer. The purchase authorization request contains Information about the merchandise to be purchased, identifying information about the proposed purchaser, some of which is the identifying information Assigned by the ISP to the subscriber. The ISP confirms internally that the subscriber is still signed in to the ISP computer system by verifying the identity of the computer currently actively communicating through the IP address. When satisfied that the subscriber is still online, the ISP computer generates and sends a message to the subscriber's computer requesting confirmation of the order for the merchandise. Upon receipt from the subscriber's computer of the merchandise. Confirmation, the ISP generates and transmits to the vendor's computer a message confirming the order and providing a confirmation number, agreeing to pay the invoice which the vendor's computer subsequently generates and Presents to the ISP computer. ISP computer then uses the subscriber's credit card information and presents an invoice against the credit card account to be Sent through normal channels.	computer-specific identification confirmation system for use in a secure electronic purchasing system, or other secure electronic transaction systems like authenticating, access permission, etc. [0021] It is indeed a further object of the present invention to provide a method for encoding downloadable data or data content files, including but not limited to MP3 music files, graphic files, e-books, medical records, government databases such as tax return information and the like so that the files can only be accessed by the actual purchaser of the file and preferably only from the computer to which they were downloaded, or to a limitable number of secondary authorized devices. (Summary of the Invention) P22 The objectives and others not specifically enumerated herein are achieved by the invention disclose herein which comprises a system and a method for providing transfer of a deliverable which may be goods and services or may include information, data or anything else to a recipient who meets the selected criteria. In the case of goods and services, the recipient may be a trustworthy purchaser who provides, through the system, a commitment for payment to an on-line vendor for services or goods provided to an on-line user. In the present invention the recipient will receive the deliverables without having sensitive identifying information such as credit card information passing over the public and unsecured Internet. The system and method of the present invention provides added security and comfort of knowing that an independent, uninterested third party is confirming the identities of the parties involved and the validity of each and every transaction, in real time and the further security of knowing that at no time is the user's critical information, such as credit card information, being exposed over the World Wide Web	P 20 P 21 P 22
The present invention relates to a method for	A system for permitting a secure electronic	

implementing secure purchases over a computer network. More particularly, the method relates to a system which permits purchases of merchandise to be made over a computer network, whereby the purchaser may feel confident that personal credit card information is not at risk of being stolen and the merchant may be more confident that the purchaser is bona fide. Note: There is actually no abstract in the provisional filing and we applied " field of invention " instead.	transaction on a network is disclosed. The network has a user device having a fingerprint, a provider's server and a means for providing verification of user's identity. In response to a request by the provider's server the means for providing verification positively identifies the fingerprint of the user device. It thereupon requests a confirmation from the user device of the transaction and upon receiving the confirmation completes the transaction.	Abstract:

Application number: 09/396005 **Art Unit:** 3621
Applicant: Khai Hee Kwan **Examiner:** David Q. Le
Title: Method, apparatus and program to make payment in any currencies through a communication network system using prepaid cards

5

10

PRINTOUT RESULTS FROM OUR PLAGIARISM SOFTWARE ANALYSIS

15

Underline and italics means common matter identified

Appendix 2

Intern'l Class:

G06F 017/60 Foreign Application Data Date Code Application Number

Jul 31, 2000

WO

01/09756

Jul 31, 2000

US

PCT/US00/21058 Claims

What is claimed is:

1) A system for permitting a secure electronic transaction on a network, said network comprising a user device having a fingerprint, a provider's server and further comprising a means for providing verification of user's identity, whereby in response to a request by said provider's server said means for providing verification positively identifies the fingerprint of the user device, requests a confirmation from said user device of said transaction and upon receiving said confirmation completes the transaction.

2) The system according to claim 1 wherein the network is a public network.

3) The system according to claim 2 wherein the user device is a computer.

4) The system according to claim 2 wherein the user device is a cell phone.

5) The system according to claim 2 wherein the user device is a television.

6) The system according to claim 2 wherein the user device is a means for accessing the Internet.

7) The system according to claim 2 further comprising one or more tool box servers which identifies the fingerprint of the user device.

8) A system for permitting a secure electronic purchase transaction on a public computer network, said network comprising a user's computer, a vendor's server, and further comprising a means for providing verification of user's identity, whereby in response to a request by said vendor's server said means for providing verification positively identifies user's computer, requests a confirmation from said user's computer of said transaction and upon receiving said confirmation provides vendor's server with a means for receiving payment.

9) The system according to claim 8 further comprising a creditor's server which receives a request from a vendor's server for a commitment to pay and issues vendor's server a commitment for payment.

10) A system in accordance with claim 9, wherein said means for providing verification is a toolbox server that positively identifies user's computer by first accessing said user's computer via a gatekeeper.

11) A system in accordance with claim 10, wherein said toolbox server transmits to said gatekeeper a pair of identification numbers, wherein the first of said identification numbers is for gaining admittance and

the second of said identification numbers is for priming said gatekeeper for admittance on a subsequent occasion.

12) The system according to claim 11 wherein said tool box server and said vendor server are the same.

13) The system according to claim 11 wherein said creditor server and said toolbox server are the same.

14) In a computer network, a system for performing a secured transaction between a user's computer, and a vendor's server wherein said user's computer has received fingerprint programming from said vendor's server for creating a digital fingerprint for use by said vendor's server to identify said user's computer.

15) The computer network according to claim 14 wherein said vendor server further comprises a creditor server and a toolbox server and wherein said toolbox server issues the fingerprint programming for creating a digital fingerprint for use by said creditor server.

16) A method for performing secure electronic transactions on a network, said network comprising a user device, and a provider server, said user device having a gatekeeper and digital fingerprint stored therein, said method including the steps of: said user device sending a request to said provider server to obtain a deliverable, which request includes a user identification code associated with said user device and known to said provider server, said request initiating the transmission of a pre-arranged handshake and primer to said gatekeeper, whereupon said gatekeeper allows confirmation of said digital fingerprint.

17) A method *for* performing secure electronic transactions on a computer network, said network comprising a user's computer, a vendor server, a creditor server and a toolbox server, said user's computer having a gatekeeper and digital fingerprint stored therein, including the steps of. *i)* said *user* computer sending a purchase request to said vendor server to pay for a purchase, which purchase request includes a user identification number associated with said user computer and known to said toolbox server, said request initiating the transmission of a confirmation request from said vendor server to said toolbox server to confirm said user computer's identity; ii) said confirmation request causing said toolbox server to send a pre-arranged handshake and primer to said gatekeeper, whereupon said gatekeeper allows said toolbox server to request confirmation of said digital fingerprint.

18) A method in accordance with claim 17; wherein said primer comprises a pre-arranged handshake for the next succeeding occurrence of a transaction confirmation operation.

19) A method in accordance with claim 17. wherein said digital fingerprint is internally confirmed by said user's computer when said purchase request is initiated.

20) A method in accordance with claim 17, wherein said users purchase request is sent to said vendor substantially simultaneously with said confirmation request, which confirmation request is sent directly from said user computer to said toolbox server.

21) A system for verifying the identity of a client computer requesting access to a secured database via a *public* computer network, said network comprising a *user's* computer, *a vendor's server,* and further comprising a toolbox server for providing third-party verification of user's identity, whereby in response to a request by said vendor's server said toolbox server positively identifies user's computer, requests a confirmation from said user's computer of said request for access and upon receiving said confirmation provides vendor's server with a gatepost for permitting said client computer access to said secured database.

22) A system for permitting a secure electronic purchase transaction on a public computer network without passing credit account information over said public computer network, said network comprising

a user's computer, a vendor's server, a creditor's server, and further comprising a toolbox server for providing third-party verification of user's identity, whereby in response to a request by said vendor's server said toolbox server positively identifies user's computer, requests a confirmation from said user's computer of said transaction and upon receiving said confirmation provides vendor's server with a gatepass for receiving a payment commitment from said creditor server.

23) A system for copy-protecting content files downloadable from a computer network, said network including a user's computer, a vendors server, and a toolbox, wherein said users computer has received fingerprint programming from said toolbox for creating a digital fingerprint for use by said toolbox to identify said user's computer, and further comprising said vendor server encoding said digital fingerprint into said content files, whereby said downloaded files will only be downloadable by said user.

24) A system for copy-protecting content files downloadable from a computer network in accordance with claim 24, wherein said downloaded files can only be played on a user computer having the digital fingerprint encoded into said file by said vendor server.

25) A system for copy-protecting content files downloadable from a computer network in accordance with claim 24, wherein said downloaded files can only be copied a limited number of times directly from said user's computer onto other secondary devices, said limited number being determined by said digital fingerprint encoding.

26) A system in accordance with claim 8, wherein a said confirmation request is contemporaneously sent to a cellular device.

27) A system for performing secure electronic transactions on a computer network, said system comprising a user's computer, a vendor server, a creditor server and a toolbox server, said user's computer having a gatekeeper and digital fingerprint stored therein, and wherein when said user computer sends a purchase request to said vendor server to pay for a purchase, said purchase request includes a user identification number associated with said user computer and known to said toolbox server, said request initiating the transmission of a confirmation request from said vendor server to said toolbox server to confirm said user computer's identity; and wherein said confirmation request causes said toolbox server to send a pre-arranged handshake and primer to said gatekeeper, whereupon said gatekeeper allows said toolbox server to request confirmation of said digital fingerprint.

28) A system in accordance with claim 27; wherein said primer comprises a pre-arranged handshake for the next succeeding occurrence of a transaction confirmation operation.

29) A system in accordance with claim 27. wherein said digital fingerprint is internally confirmed by said user's computer when said purchase request is initiated.

30) A system in accordance with claim 27, wherein said users purchase request is sent to said vendor substantially simultaneously with said confirmation request, which confirmation request is sent directly from said user computer to said toolbox server.

31) The system according to claim 2 wherein the user device is a digital set top box connected to a television.

32) The system according to claim 1, wherein said fingerprint provides an electronic signature that can be used to identify a user. Description

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims priority on WO 01/09756, PCT/US00/21058 filed Jul. 31, 2000.

The present application also claims the priority of the following U.S. patent applications: U.S. application Ser. No. 09/523,902, filed Mar. 13, 2000, which is a continuation in part of U.S. application Ser. No. 09/500,601, filed Feb. 8, 2000 and claims the benefit of priority to U.S. Provisional application Ser. No. 60/167,352, filed Nov. 24, 1999 and U.S. Provisional application Ser. No. 60/146,628, filed Jul. 30, 1999. The specifications of these applications are hereby incorporated herein by reference in their entireties.

FIELD AND BACKGROUND OF THE INVENTION

[0002] The present invention relates to *systems and methods* for implementing secure transactions including but not limited to purchases over a computer network. More particularly, the *methods described herein relate to* a system which permits *users of* a network to perform transactions such as banking, purchases of merchandise and/or services and other transactions to be made over a computer network, whereby the purchaser may feel confident that information including but not limited to private personal information such as credit card or other payment information is not at risk of being diverted, misappropriated or stolen and the *vendor* may be more confident that the purchaser is bona fide.

[0003] The *present* invention *permits one or more parties to a transaction* to *have confidence that the other party* to the transaction is who he or she purports to be. This may be accomplished by the use of a "fingerprint" of the computer or other device used by such party and/or the use of a one time password. The fingerprint of the computer or other device used for the transaction provides significant security for parties to a transaction. If additional security is desired or if for example the computer or other device used in the transaction is not secure and available for use by third parties a one time password may also be used. The one time password concept of the present invention changes the password every time a request for authentication is made so that the next time the user of the computer or other device is the subject of an authentication request, the new password is required for this authentication and a new password is generated for the subsequent request. The one time password is described in further detail below.

[0004] It is well known for members of the public to access the global client/server network commonly referred to as the Internet, a part of which is the World Wide Web, for the purpose of searching for and purchasing merchandise from on-line vendors selling wares ranging from travel services and investment services to buying CD recordings; books, software, computer hardware and the like. Numerous patents teach methods or systems purporting to secure commercial credit card transactions carried out over the Internet. Examples of such patents include U.S. Pat. Nos. 5,671,279 to Elgamal, 5,727,163 to Bezos, 5,822,737 to Ogram, 5,899,980 to Wilf et al. and U.S. Pat. Nos. 5,715,314 and 5,909.492, both to Payne, et al-, the disclosures of which are incorporated by reference herein.

[0005] Most of the disclosed systems have the disadvantage that they rely on the transmission of sensitive information over unsecured network routes and lines for each transaction. Although practically speaking, the systems which rely solely on encryption are fairly safe, there is still some risk of credit card misappropriation and there is little psychological comfort given to potential users by their knowing that encryption is being used. In addition, the merchant does not know whether the person making the purchase is actually the person whose name is on the credit card

[0006] Generally speaking, the Internet is a network of computers, remote from one another linked by a variety of communications lines including telephone lines, cable television lines, satellite link-ups, wireless networks and the like. Internet service providers (hereinafter "ISPs") provide the link to the main backbone of the Internet for small end users. The account for the end user is established in the normal manner usually by providing credit card information to the ISP by conventional means, such as by voice telephony, fax transmission or check. In most ISP-end user relationships, the ISP has been given credit card *or other credit account* information, which information is on file with the ISP and available to the ISP's computers. In return for receiving payment, the ISP provides a gateway to the Internet for the

end-user's use. The end-user (or *user)* is provided with Identification codes for dialing directly into the ISP's computers and software means (for example, dialer software, browser software, electronic mail software, and the like) for doing so if necessary.

[0007] Most purchases are conducted in the following manner: a purchaser using a browser application on his local client computer connects via his computer's modem to a dial-up Internet Service Provider (hereinafter "ISP") and makes connections through the ISP to various Web sites, i.e. Internet server locations assigned a URL (Uniform Resource Locator) address. The purchaser selects his merchandise and the vendor *usually* requests payment by one of several methods, one of which *may include* payment by providing credit card information.

[0008] According to surveys and other marketing data, there always has been and there still exists a high percentage of the population which is deterred from purchasing merchandise directly over the *Internet.* This large percentage of the population apparently fears that, despite all the efforts at security and cryptography promised by the vendors, there still exists the *possibility* that their credit account information will be intercepted on-line by a third party computer hacker and used illegally, at great expense and trouble for the cardholder.

[0009] An additional anxiety-inducing factor related to merchandising over the Internet, or e-Commerce, is that the *vendor* cannot always be certain that just because he has obtained credit card or account information, that he will actually be paid for the merchandise he ships. After all, credit card fraud and/or theft occurs regularly and may not be caught in time to stop the order from being shipped. When the cardholder discovers the theft and stops the card, it may be too late for the vendor to recover *the shipped goods.* At the very least, this situation leads to unnecessary aggravation and wasted resources for the *vendor,* credit card company and cardholder.

OBJECTS OF THE INVENTION

[0010] Thus, it is an *object* of the present invention to provide a system and method for implementing secure transactions including but not limited to purchases over a computer network.

[0011] It is another object of the invention to provide a system and method for permitting users of a network to perform transactions such as banking, purchases of merchandise and/or services and other transactions to be made over a computer network.

[0012] It is an object of the invention to provide a system and method whereby the user may feel confident that information including but not limited to private personal information such as credit card or other payment information is not at risk of being diverted, misappropriated or stolen and the supplier may be more confident that the user is bona fide.

[0013] It is also an object of the present invention to provide a system and method that permits one or more parties to a transaction to have confidence that the other party to the transaction is who he or she purports to be.

[0014] It is a still further object of the invention to provide a system and method whereby a "fingerprint" of the computer or other device used by a party to a transaction is used for security purposes.

[0015] It is another object of the invention whereby a one time password may be used to provide security for a transaction.

[0016] It is an objective of the present invention to provide a system and method for on-line purchasers of merchandise marketed over the Internet to pay for those purchases with minimized exposure to the

risk of billing information theft by electronic interception.

[0017] It is an objective of the present invention to provide a system and method for on-line *purchasers* of merchandise marketed over the Internet to pay for those purchases *with minimized* exposure to the risk of credit card theft by electronic interception.

[0018] It is a further objective of the invention to provide a mechanism for facilitating e-commerce which will increase the confidence of the consuming public in the safety of such transactions.

[0019] It is *still* a further objective of the invention to provide a mechanism for facilitating e-commerce which will increase the confidence with which vendors may ship the purchased product or deliver the purchased service without fear of the payment being provided fraudulently.

[0020] It is yet a further object of the present invention to provide a site-specific and computer-specific identification confirmation system for use in a secure electronic purchasing system, or other secure electronic transaction systems like authenticating, access permission, etc.

[0021] It is indeed a further object of the present invention to provide a method for encoding downloadable data or data content files, including but not limited to MP3 music files, graphic files, e-books, medical records, government databases such as tax return information and the like so that the files can only be accessed by the actual purchaser of the file and preferably only from the computer to which they were downloaded, or to a limitable number of secondary authorized devices.

SUMMARY OF THE INVENTION

[0022] The objectives and others not specifically enumerated herein are achieved by the invention disclosed herein which comprises a system and method for providing transfer of a deliverable which may be goods and services or may include information, data or anything else to a recipient who meets the selected criteria. In the case of goods and services, the recipient may be a trustworthy purchaser who provides, through the system, a commitment for payment to an on-line *vendor* for services or goods provided to an on-line user. In the present invention the recipient will receive the deliverable without having sensitive identifying information such as credit card information passing over the public and unsecured Internet. The system and method of the present invention provides added security and comfort by providing, among other features, the comfort of knowing that an independent, uninterested third-party is confirming the identities of the parties involved and the validity of each and every transaction, in real time, and the further security of knowing that at no time is the user's critical information, such as credit card information, being exposed over the World Wide Web.

[0023] In one embodiment, the method takes advantage of an existing relationship between the recipient with one or more computers/servers belonging to a provider or a third party working with either the provider or the recipient linked by a variety of communications lines including telephone lines, cable television lines, satellite link-ups a wireless network and the like. An account for the recipient is established usually by providing identifying information to a provider. The recipient is provided with identification codes for *dialing* directly into the *provider's* computers and software means (for example, dialer software, browser software, electronic mail software, and the like) for doing so if necessary. Each time a user signs in to the provider's computers for an on-line session, the user is assigned an identifying code or address. The *recipient's* computer transmits messages which are received by the *provider's computer. During the entire time* the *on-line session in progress, the identifying code or* address does not change and is thus available as identifying information. By monitoring and occasionally reverifying that the *user's* computer is still on-line at the assigned address, the *provider* can confirm that certain activities could be attributed to the *user.*

[0024] One example of this process would be when a bank customer wants to be authenticated to log into his or her bank account. The authentication would be done after the user has connected to the Internet through his or her ISP or other network and goes to the bank's website or other database to access personal information. The user would be authenticated by the present invention prior to being allowed access to the financial information.

[0025] In another-exemplary embodiment, the method *takes advantage of* the *existing* business relationships between the end user with the owners of member computers/servers who give access to the *backbone* structure of the Internet. *As explained hereinabove,* the Internet is a network of *servers,* remote from one another linked by a variety of communications lines *including telephone lines, cable television lines,* satellite link-ups and the like. Internet service providers (hereinafter *"ISPs")* provide the link to the main backbone of the Internet for small end users. The account for the end user is established in the normal manner usually by providing credit card information to the ISP by conventional means, such as by voice telephony, fax transmission or check. In most ISP-end user relationships, the ISP has been given credit card *or other credit account* information, which information is on file with the ISP and *available* to the ISP's computers. In return for receiving payment, the ISP provides a gateway to the Internet for the end-user's use. The end-user (or subscriber) is provided with identification codes for *dialing* directly into the ISP's computers and software means (for example, dialer software, browser software, electronic mail software, and the like) for doing so if necessary.

[0026] Each time a user signs in to the ISP's computers for an on-line session, the *user is assigned* an Internet Protocol (hereinafter "IP") address. The *user's* computer transmits messages which are received by the ISP computer and relayed through the IP address and out onto the Internet to the ultimate intended recipient computer. During the entire time the on-line session in progress, the IP address does not change and is thus available as identifying information. By monitoring and occasionally re-verifying that the *user's* computer is still on-line at the assigned IP address, the ISP can confirm that certain activities could be attributed to the *user.*

[0027] In another embodiment of the *invention, where a transaction* is to take place a user logs into a network which may be the Internet or some other public or private network, LAN or WAN. When the user accesses the desired location whether it be a website or other location the fingerprint of the computer or other device that accessed location takes a finger print of the user's device. This fingerprint may be of the device's hardware and/or software and/or other attribute that may provide a unique definition. This fingerprint may be used throughout the initial transaction to make sure that the device online continues to be the same device or the fingerprint may be a signature for use in other transactions from that device.

[0028] A further embodiment of the present invention takes advantage of the relationship which is re-created every time an Internet *user's* computer goes online and signs into his ISP's computer by assigning to the ISP computer the function of clearinghouse and active intermediary between the *user's* computer and *the* vendor's computer. A *user* computer signs in to the ISP computer system and is recognized and *assigned an IP address. When the user* identifies merchandise or services at a vendor's website which he wishes to purchase, he sends programming to the website which selects the items and instructs the vendor's computer to generate a purchase authorization request which is sent to the ISP computer. The *purchase authorization request contains* information about the *merchandise to be purchased, identifying information about* the *proposed purchaser, some of which is* the *identifying information assigned by the ISP to* the *user.* The ISP *computer confirms internally that the user* is still signed in to the ISP computer system by verifying the identity of the computer currently actively communicating through the IP address. When satisfied that the *user* is still online, the ISP computer generates and sends a message to the user's computer requesting confirmation of the *order for the merchandise. Upon receipt from* the *user's computer of* the *confirmation,* the ISP generates and transmits to the vendor's computer a message confirming the order and providing a confirmation

number, agreeing to pay the invoice which the vendor's computer subsequently generates and presents to the ISP computer. *The* ISP computer then uses the *user's* credit card information and presents an invoice against the credit card account to be sent through normal channels.

[0029] In another exemplary embodiment of the present invention, the ISP does not serve as the credit giver or transaction verifier/guarantor. This function is provided by a bank or vendor with whom the user already has a credit account, and who has an online presence, i.e. has a transaction server connected to the Internet which can participate in the transaction as it is carried out by the user/consumer.

[0030] Another aspect of the present invention lies in the security provided by employing a method for verifying that the system is only usable by computers specifically registered with the system. More particularly, the method for identifying a registered computer, i.e. one which can be used for making a purchase transaction, or other electronic transaction and/or request, on the system of the invention, is constructed such that if a hacker were to try to "pretend" that his computer was in fact the registered computer of a bona fide user, the codes detect that they are no longer in their originally installed environment and the user's identity becomes inoperable. The system can only be reactivated by re-registering the machine.

[0031] In another aspect of the present invention, the system is configured such that the request for a confirmation of a purchase transaction, or other electronic transaction, is forwarded in the form of an SMS (short message system) note to a user's cellular communications device, such as a cellular phone, alphanumeric pager or modem-equipped handheld computer. Thus, if the user was not sitting at the system registered computer, he can still be advised instantly that someone else, perhaps illegally, is attempting to fraudulently use his account or even his computer to make a purchase. This feature of the invention can contribute to deterring such computer fraud.

[0032] In a still further embodiment of the present invention there is a system and method of performing secure transactions by the use of a one time password. In this embodiment, there are two different passwords. The first is a login password. This password is always the same unless changed by the user. The login password and the fingerprint decrypt a one time password that may be used to secure a transaction. The combination of the login password and the fingerprint permits the user to receive an encrypted, one time password and decrypt it. This password is changed for each transaction and is not repeated, thus providing superior security for a given transaction.

BRIEF DESCRIPTION OF THE DRAWINGS

[0033] For a better understanding of the invention, the following drawings are included for consideration in combination with the detailed specification which follows:

[0034] FIG. 1 shows a *user* computer in communication with a vendor computer via the ISP computer, wherein *user* computer is initiating a purchase transaction;

[0035] FIG. 2 shows the vendor computer communicating with the ISP computer to request authorization to complete *user's* requested transaction;

[0036] FIG. 3 shows the ISP computer confirming that correct IP address is active with *user's* computer and requesting confirmation of *user's* transaction;

[0037] FIG. 4 shows *users* computer responding to ISP computer's request for confirmation;

[0038] FIG. 5 shows ISP computer's transmission of a confirmation code and invoicing instructions to vendor's computer;

[0039] FIG. 6 shows a block diagram illustrating another exemplary embodiment of the present invention;

[0040] FIG. 7 shows a block diagram illustrating another exemplary embodiment of the present invention;

[0041] FIG. 8 shows a block diagram illustrating another exemplary embodiment of the present invention;

[0042] FIG. 9 shows a block diagram illustrating the handshake and priming process of the system of the present invention:

[0043] FIG. 10 shows a user reacting remotely to fraudulent use of his PC;

[0044] FIG. 11 shows a user computer in simultaneous communication with a vendor computer and the AA computer, wherein user computer is Initiating a purchase transaction; and

[0045] FIG. 12 shows a block diagram illustrating another exemplary embodiment of the present invention.

DETAILED DESCRIPTION OF THE EXEMPLARY EMBODIMENTS

[0046] In all of the exemplary embodiments which will be described hereinbelow, there are certain common features which, together with reference to the drawings, will be described once here to provide the reader with an easily understood framework.

[0047] Many devices today have unique hardware fingerprints. For example, the identity of the processor, its type and clock speed, the hard drive manufacturer, the size of the hard drive, the amount of Ram, etc., all combine to make each device relatively unique. Other devices have similar fingerprints or can be provided with such relatively easily. These products include cell phones, PDA's televisions web accessing apparatus and other devices commonly available. These fingerprints can be combined with a user identifying code so that a purveyor of goods or services can have increased assurance of the bona fides of the person using this equipment to buy these goods and service or access information..

[0048] As was discussed above, the present invention takes advantage of *an existing* relationship between the user or recipient with one or more computers/servers belonging to a provider or a third party working with either the provider or the recipient. These computers/servers are linked by a variety of communications lines including telephone lines, cable television lines, satellite link-ups a wireless network and the like. An account for the recipient is established usually by providing identifying information to a provider or a third party. The recipient is provided with identification codes for dialing directly into the provider's computers and software means (for example, dialer software, browser software, electronic mail software, and the like) for doing so if necessary. Each time a user signs in to the provider's computers for an on-line session, the user is assigned an identifying code or address. These codes may be assigned by the provider, a third party or an ISP. The recipient's computer transmits messages which are received by the provider's computer. During the entire time the on-line session is in progress, the identifying code or address does not change and is thus available as identifying information. By monitoring and occasionally re-verifying that the user's computer is still on-line at the assigned *address,* the provider can confirm that certain activities could be attributed to the user.

[0049] Alternatively, instead of relying on the presence of the identifying code or address of an ISP provider, the provider's device such as a computer or server takes a fingerprint of the user's device. This fingerprint can be of the device's hardware, software or other attribute and combinations thereof. If the

provider's computer desires to ascertain whether the user is still the same user in an extended transaction or the same user in a previous transaction, the fingerprint can be taken and compared to an earlier fingerprint

[0050] The present invention is designed to reduce compromising the security of one's accessing information which may for example be credit account information or other relevant information which can be caused by transmitting the information over the unsecured World Wide Web. Additionally, the invention helps to ascertain that the parties participating in a transaction are who they purport to be. The exemplary embodiments assume the following arrangement of the parties to a transaction:

[0051] [a] a user is connected via his PC or client to the Internet through telephone, cable TV, satellite or data lines, usually through a modem and the user's client PC has installed therein a browser program. such as Microsoft Corporation's Internet Explorer or Netscape Corporation's Navigator or Communicator, an instance of which has been activated prior to the transaction;

[0052] [b] a vendor has a server in communication with the Internet which constitutes or communicates a Website accessible to users' browser,

[0053] [c] a security administration system operates via a security server, or toolbox (hereinafter `TB"), the physical location of which can vary as will be discussed below; and

[0054] [d] a creditor or payment guarantor has a payment server, although this function may optionally be performed by the security server. In the context of the present application, it should be understood that reference to a client or PC expressly includes any browser-equipped telecommunications device which gives the user the ability to access and interface with remote servers, and in particular Web sites on the Internet. Thus, such devices include browser-equipped cellular phones, personal digital assistants, palm held computers, laptop computers, and desktop PCs, though not exclusively.

[0055] Additionally, it should be noted here that, rather than being a vendor of merchandise, vendor might simply be a provider of an information or financial service, as example. Thus vendor might be using the present invention to ensure that access to secured databases is only to properly authorized and duly-identified persons.

[0056] All of the four components of the system employ a combination of security measures, for instance, all transmissions preferably take place in an encrypted environment, such as RSA, Triple DES, etc., using encryption tables which are replaceable by the security server or by a central system administrator server at random intervals.

[0057] The systems are of two general kinds; where the ISP will participate in the system, giving the highest possible level of security, and where the ISP is not a participant in the system. Where the ISP is a participant, it can participate in three aspects;

[0058] [1] the ISP is a mere intermediary of the communications between the recipient and the provider,

[0059] [2] the ISP can serve as the physical host of the TB and

[0060] [3] the ISP can be the creditor or payment guarantor, since the ISP already has an ongoing service agreement with the user.

[0061] Where the ISP is not a participant as a creditor or payment guarantor, this function can be served by another party. In this instance the ISP may have no function at all. An example of this situation would be a LAN or a WAN which may be either public or private. There can be any suitable provider who performs a function at the request of the user and receives some consideration in return or enables

collection of compensation for a third party. The advantage to having the ISP as participant wherein the TB is physically at the site of the ISP has been alluded to above. That advantage lies in the fact that since most users dial into an ISP's modem basket over copper phone lines, the only way for a hacker to get between the ISP server (and the TB if installed piggyback to the ISP server) and the user is to physically tap into a phone company junction box, something that most hackers are not likely to do. Even if the TB is at another physical location, the system still retains effectiveness but the fewer areas open for hacker attack, the better. If the ISP is not a participant, insofar as being a creditor or payment guarantor, this function can be fulfilled by the Internet-accessible payment servers of such business entities as online banks, merchants which give their customers credit accounts and other credit-providing institutions. In such a case, the TB might be located at the site of the credit institution, or in fact a single server could act as the TB as well as the payment server. In another case, the TB and the payment server might be at completely different locations.

[0062] Before a transaction can take place, the components of the system need to be programmed and/or installed as follows:

[0063] The TB is at least on server and preferably a series of at least three servers and in addition a Firewall Server. The TB also may contain a database comprised of all of the security system's user participants. Additionally, TB can include programming to check and update the recipient or user's software version, and encryption tables and instructions to either update those tables as needed, mark them for future updating or to direct user's browser to the URL of an appropriate server, such as the central administrator server for downloading updated tables. The vendor server is modified such that a button or other directing device is added to the purchase initiating software that gets downloaded to a users browser from the vendor server when a user indicates readiness to commit to a transaction such as to pay for a transaction. The added button tells a user to click on it if payment by the secured system of the invention is desired. By clicking the button, the user initiates a series of events which will be described further below.

[0064] The creditor server is provided with programming directing it how to respond to the request from a vendor server for payment on a transaction that is accompanied by a Gatepost code, which the vendor receives from the TB. The TB records all transaction data and assigns a unique transaction ID (UTID) to the record and further marks the record as "not yet confirmed". TB records the transaction data received from the vendor server and puts it under a URL. TB then commands User's waiting thread to come and retrieve the page at the URL on the TB and show it to User. The shown page is the Confirmation Request page which appears to user on client PC as a Pop Up window.

[0065] In the Pop Up window, User sees certain details of the transaction and text to the following effect "We have been asked to pay a vendor 517.20 for an order from you. Do you approve the transaction?". To approve the transaction, User is instructed to input his System password (selected in the registration process) and click the OK button.

[0066] a) If the User clicks Reject or does not respond within a predetermined time frame then the order is deemed not accepted and TB rejects Vendor's request for payment URL.

[0067] b) If the User accepts the transaction by entering his personal password into the appropriate field and clicking the OK button the client software closes the confirmation request window and decrypts a one time password using a key generated from the personal password and sends it back to the TB.

[0068] c) In one exemplary embodiment of the present invention, the User can elect to additionally receive notice on his phone or other communication device preferably a cellular phone or other cellular-enabled device (such as an alphanumeric beeper or an Internet-ready personal digital assistant or PDA) of the transmission of a Confirmation Request page to his PC. When User has elected this service, the transmission to his PC of a Confirmation Request page is accompanied by the simultaneous

transmission of an SMS (Short Message System) message to his cellular device, thereby advising him that someone is operating his PC and conducting a purchase transaction. Using this follow-me technology, a user might then use his cellular device to respond to the SMS message with a message to cancel the transaction and/or initiate a trace of the fraudulent purchase request.

[0069] The transaction continues as follows in the embodiment wherein the Toolbox is located at the vendor or at the secure administration site, for example. Physical Placement of TB in an exemplary embodiment of the invention, the TB is at the secure administration site or at the vendor site. In the case of the TB being at the vendor site, the TB is locally connected to the service provider's server. The user is not necessarily purchasing merchandise, but, for example, is making a request to the vendor server for access to secured databases contained therein or protected thereby. Thus, in order to be certain that the user is who he claims to be the user is forwarded to the TB server to be authenticated. The rest of the procedure is substantially the same as described above.

[0070] As noted above, rather than being a vendor of merchandise, vendor might simply be a provider of an information or financial service, as example. Thus vendor might be using the present invention to ensure that access to secured databases is only to properly authorized and duly-identified persons. For example, a bank might want identity verification before permitting a customer access to his account information or to use financial services. As another example, a large corporation might use the present invention to give third-party verification of an employee's or outside contractor's identity before permitting them access to secured databases which might not otherwise be available via the Internet.

[0071] The TB may be, for example, a mini-server, dedicated to the security tasks assigned to it. The TB is provided with programming which, when activated, sends, receives and verifies the proper forms and/or data to either a participating home user, ISP server or vendor in order to carry out the proposed transaction.

[0072] The authentication agent (hereinafter "AA"), may be software downloaded into the client computer, AA, which will be further described below. The AA generally performs the same function as a magnetic strip on a plastic card, e.g., a credit card. This enables the AA to be employed in internet generated automatic teller machine (ATM) applications, such as fund transfers, credit card or debit card credits or debits, without the need for physical access to the ATM.

[0073] The procedure described in this embodiment above is described as follows.

[0074] 1) In one embodiment of the present invention, AA sends SIMULTANEOUS messages to vendor and TB, so that the TB is expecting a certain message from the vendor.

[0075] 2) The AA's action is described below. In the present embodiment the AA is a COM object which creates a "digital fingerprint" consisting of various identifying hardware characteristics which it collects from the user's PC, as well as passwords (to be described further). Activation of the account initiates a process by which the TB records a fingerprint for the user, which the AA has derived, including a unique identification ("UID") for the user, using the identifying characteristics of user's PC (e.g CPU ID number, hard disk serial number, amount of RAM. BIOS version and type, etc-).

[0076] 3) When a transaction starts, the user's AA, which is a simple DLL, is activated by the vendor script. The AA sends a message to the Toolbox server, using the server's public key. If the server answers the AA, the home user's computer knows that it is talking to the correct server, since only the Toolbox has the private key that can decrypt the message sent with its public key. The Toolbox server now sends the user half of a new Triple DES key that it has generated so that the home user can communicate with it securely. Next the TB asks for the user's OTP (one time password) which is stored on a configuration file in the home user's computer. This configuration file can only be opened by a combination of personal password and CPU id. If the home user's computer responds with the correct

password, the TB knows it is talking to the correct user. Once the TB has verified that it is talking to the correct user, the TB sends a dynamically generated smart DLL to collect the computer's hardware signature, verifying that it is also talking to the correct machine. The TB also records the number of encounters with the user. Any hacker who manages access probably fails this check, and is thereby discovered. The configuration file, which contains the account ID, machine ID, and a replaceable one-time password, among other items, can be stored or on the hard drive or on a removable floppy, i.e., the configuration file can be removed and taken away from the proximity of the user's computer, thereby disabling the user's access to the account from that computer. When registering for the first time, and also when authenticating a user, the simple DLL loads itself into memory, and calls a "smart" DLL, from a collection of thousands of continuously regenerated smart DLL's, which collects a large number of different parameters, for example 12, identifying the user's computer. A simple example of an authentication transaction is now described using two machine parameters. The DLL applies an algorithm such that if the disk serial number is 1 and is multiplied by 1; and if the CPU serial number is 2 and is multiplied by 2, the resulting string is their sum or "5". Thus, 1(1); 2(2)=5. This information is hashed by the DLL according to that DLL's hashing programming, then encrypted, and the encrypted hash is sent back to the TB. The order of the parameters and the algorithm used can change each time. Furthermore, the actual information is further interspersed with "garbage" code, expected by the TB, every time. The server receives the hashed and encrypted result from the smart DLL, and compares it to the result which it expects to receive. This is done by the TB by calculating the expected result by running it's own copy of the unique DLL on the user's identifying parameters that it has stored in the database. It then hashes the result, and compares its hash to the de-encrypted hash string it received from the user.

[0077] An exemplary embodiment of the present invention, more specifically uses a 2048 bit RSA key to initiate the handshake, and thereafter moves to Triple DES encryption. The Public Key is distributed to all the end-users with the Agent and the Private Key(s) are held by the AA Server There is a different set of Keys for different Providers, i.e., Credit Card Companies, Banks, etc.

[0078] The TB can be used to verify a digital fingerprint in various forms of Internet transactions, for example:

[0079] Banking and Financial Services

[0080] A bank or financial institution can use digital fingerprints to provide customers with secure access to their accounts for stock transactions and account management. Customers can use their digital fingerprints as a universal log-in at the bank's Web site for quick access to their account information without having to remember a unique log-in name and password. To further enhance each user's experience, the bank can provide targeted content and services to its customers based on the registration information contained in their digital fingerprints. The bank can also use digital fingerprints to send secure e-mail, allowing it to pro-actively send private account information to its customers.

[0081] In an alternative embodiment, the present invention may be used to help track down credit card fraud. If a computer has been used for certain transactions where the credit has been rejected for various reasons the fingerprint can be used to create a database so that future purchases from that location may be subjected to greater scrutiny. In another embodiment that has applicability not only in the banking and financial services industry is the use of the present invention to provide an electronic signature. Secure electronic signatures are increasingly sought to provide both the customer and a provider with security. Electronic signatures are becoming more important in many banking and financial transactions as well as in other areas where a traditional signature is required such as contracts and other legal types of documents. The security features of the present invention may be used to provide a secure electronic signature that the recipient will have confidence as to the bona fides thereof.

[0082] Retail

[0083] A manager of an online retail store can watch customers browse merchandise, identify purchase patterns, observe the behavior of casual visitors, and set up accounts for purchases. A manager of a retail Internet site can perform these same functions online by using digital fingerprints. By implementing client authentication with digital fingerprints, the retail site can analyze customer interests and behaviors, track and compare the profiles of visitors who browse and those who actually place orders, and perform market analysis and segmentation based on information presented in its customers'digital fingerprints. The site can extend the power of digital fingerprints by linking the ID to information in its existing customer database (e.g. customer's account, order status, or purchase history).

[0084] Additionally, by using the one-step registration feature of digital fingerprints, the site can quickly find out information about first-time visitors to the site. The site can use this information to provide relevant content to these visitors, thus capturing their interest and increasing the likelihood that they will become customers. The authentication and security associated with digital fingerprints can allow the site to verify the identity of a customer, eliminating consumer misrepresentation and false orders. Additionally, consumers will have more confidence in conducting transactions on the Internet.

[0085] Debit Card Transactions

[0086] Currently, when someone wants to purchase something on the Internet they go to an e-commerce website and enter their personal credit card information. This information then gets sent to both the eMerchant and the card-issuing bank to verify that the customer has sufficient funds to make the purchase. Although this process checks to make sure the customer has sufficient funds, what it does not check is the card owner's identity to ensure that he is the one who is really making the purchase. This is where the present invention has significant advantages.

[0087] The system of the present invention provides the authentication necessary to verify that the true owner of the card is making the purchase and not a waiter, hacker, or a gas station attendant stealing someone's card information and online identity. When a card issuing bank issues a Visa.TM. or MasterCard.TM. debit card, the card owner goes onto the Internet and creates his digital identity. He does this by accessing the issuing banks website and downloading a small software agent. Once downloaded, a button is now located on the users browser that will allow him to make secure Internet purchases.

[0088] When a Visa.TM. or MasterCard.TM. debit card owner wants to make an Internet purchase, he would go to an eMerchant website where he would like to make a purchase. After choosing the item(s) he wishes to purchase on the eMerchant website, a user would click on checkout and will be forwarded to the checkout page of the eMerchant website. This is a typical example, and is unaffected to this point by the system of the present invention. At the checkout page, a user will need to choose a payment method. In order for a user to be approved by his card-issuing bank, he can be required to provide authentication such as by first clicking on an authentication icon located on his computer icon tray. This icon will establish a secure link with the server. The user will now proceed with the purchase as normal by choosing MasterCard.TM. or Visa.TM. depending on the card type and enters his card information for payment. Once entered, the user may click "purchase" and the eMerchant will begin to process the transaction. The processing begins with the eMerchant communicating with the card issuing bank to verify that the user has sufficient funds to make the purchase and checking to verify the user entering the card information is the actual card owner. The card-issuing bank receives the inquiry from the eMerchant and contacts the TB server to authenticate the user. The TB server then opens a pop-up window on the users PC asking him to verify that he really wants to make this purchase and requests for him to enter his username and password. Once authenticated, the TB server notifies the card-issuing bank that the user has approved the transaction and that he is the actual owner of the card. The card-issuing bank then notifies the eMerchant that the user has sufficient funds, and that he has been authenticated as the actual card owner. The eMerchant then notifies the user that his purchase has been

approved and is given an order number as a receipt. This completes the transaction in real time. The user will be disconnected from the TB server the moment he closes his web browser.

[0089] Publishing and Subscription

[0090] An online newspaper depends on advertising and subscription revenues. Digital fingerprints can allow this site to use basic registration information that is in a digital fingerprint--country, zip code, age and gender--to understand the profile of its visitor population, thereby increasing the value of the advertisement placement and the amount that can be charged for the advertisement.

[0091] The site can use the universal log-in feature of digital fingerprints for identifying its site subscribers. Site visitors no longer need to remember unique log-in names and passwords for the site, and the site no longer needs to maintain a costly log-in and password database. By understanding the profile of its first-time customers, and providing tailored information based on the basic registration information in a digital fingerprint, the site can use digital fingerprints to help it acquire new customers.

[0092] Services

[0093] A service company, such as a delivery company, can use digital fingerprints to provide secure access to its Web site. Digital fingerprints can allow this site to provide a highly customized experience to its visitors, for example, by providing specific delivery rates based on the geographic location of the customer.

[0094] Business-to-Business

[0095] With the level of authentication provided by digital fingerprints, a manufacturing company can allow portions of its Internet site to be updated by its business partners and accessed by its customers. The manufacturing company's suppliers can update their product availability and scheduled shipping date in the manufacturer's database, providing a more efficient means for inventory management. Additionally customers can track order status through the same online database. These types of transactions would not be possible on the public Internet without the use of digital fingerprints to authenticate the identity of the company's suppliers and customers.

[0096] Music, Picture, Video, or e-Book File Sale and Download

[0097] Another possible application for the unique hardware fingerprint is to use it as a lock and key for preventing unauthorized downloading. copying and playback of content files. such as MP3 music files, e-book files, graphic files, etc. The fingerprint could be associated with the downloaded file and attempting to open the file on a machine which does not bear the fingerprint results in the file being permanently locked, unusable or somehow otherwise disabled The fingerprint coding can determine whether the downloaded file can be copied to and played on a limited number of secondary machines. In fact, the encoding could initially be used to determine that the person downloading the file is the person even entitled to do so.

[0098] Cell Phone Commerce

[0099] In many areas cell phones are being used to charge goods and services just like the traditional credit card. This makes the cell phones very convenient but does raise some security problems. One of the problems with the use of cell phones is their memory. Most phones that are currently in use today display the most recent numbers inputted into the phone. These numbers may be as innocent as a telephone number but can also include account numbers and passwords. In addition, there are unscrupulous persons who can clone cell phone numbers when a user is in the vicinity. The present invention may also be used to perform secure transactions with a cell phone and avoid these security

issues. A user of the present invention can add a cellular phone to the system. The system can be used to ascertain whether the person on the cellular phone is an authorized user. In this embodiment, the user connects to a merchant in order to make a purchase. The server sends an SMS message to the cell phone user that will ask the user to complete the message with the appropriate code. Both the illegal clone and the user's phone will receive the request for the code. The user knowing that he did not seek to make a purchase can respond with an appropriate message to terminate the purchase.

[0100] Alternatively, a fingerprint of the cell phone that is being added to the system is created. When a purchase is being made, the vendor sends the SMS message and the user must respond the code that has been entered. The vendor's server checks the code for accuracy and the fingerprint as well and if appropriate, sends to the cell phone user a one time pass word. The one time password combined with the user's pin number acts as a signature for the purchase of goods or services using the cell phone.

[0101] Pay-Per-View Television

[0102] The present invention also has applicability in the field of television. Currently many cable companies and satellite television providers are using "Smart Card" type technology to restrict the viewer to programs and/or services that have been paid for. The user purchases a Smart Card from the service provider and inserts the card into the descrambler at home. As the cost of cable and satellite television programs increases there is a need to prevent users of cable systems and satellite television services from using the television set top box with more than one television and to prevent the user from loaning or giving the descrambler and smart card to a friend or relative for their use. The present invention permits the fingerprint of the television set to be ascertained and will cause the descrambler to be inoperative if the user does not have the proper television connected to the descrambler.

[0103] It will be appreciated by those skilled in the art that the present invention can be used with any number of different devices to prevent unauthorized use.

[0104] The examples discussed herein and demonstrated by the Figures are merely for illustrative purposes only. Variations and modifications of the disclosed invention in a manner well within the skill of the man of average skill in the art are contemplated and are intended to be encompassed within the scope and spirit of the invention as defined by the claims which follow.

[0105] For example, in another exemplary embodiment the ISP is not the site where the Toolbox resides. With reference to FIG. 7, The Toolbox could be physically located at the site of the credit provider ("Creditor"), e.g. online-enabled bank, credit card provider or other affinity-card or charge account provider (including brick-and-mortar retailers with an online presence such as Macy's) and in communication through normal channels with Creditors transactional server. In this case, the ISP would not be an active part of the purchase transaction, other than in the usual known way by giving User access to the Internet. Generally, except as specified below, the rest of the process proceeds substantially as described below. Specifically, in this exemplary embodiment, the account is set up as follows:

[0106] Installation Process

[0107] 1) A user requests to join the system, which could for, example be, via an ASP page on a web server, over an HTTPS connection.

[0108] 2)The applicant receives an account ID, and his application information is stored in an applicant's database on an application and database server, behind a firewall. The system owner, which can be an ISP, bank or other financial provider accesses this database from another web page, located on a Web server behind a firewall on an internal LAN.

[0109] 3)When the system owner approves the user's application, the system automatically sends the user

an email containing a link to a unique URL where he can begin the registration process. It also generates a one-time activation key linked to the user's account. The system owner must give this one-time activation key to the user in a secure way (for example, in person, or via a printout from his automatic teller). Possession of the one-time activation key constitutes proof that the user is who he purports to be during the activation stage.

[0110] 4) When the user goes to the URL, and presses the "Activate" button, the activation process begins by downloading a DLL containing a COM object to his computer. Dynamic Link Library (DLL) refers to the ability in Windows and OS/2 for executable memory to call software libraries (i.e., subroutines, or code for accomplishing specific functions) not previously linked to the executable. The executable is compiled with a library of "stubs" which allow link errors to be detected at compile-time. Then, at run-time, either the system loader or the task's entry code must arrange for library calls to be patched with the addresses of the real shared library routines, possibly via a lump table.

[0111] 5)This COM object relays the user's account ID (which it knows because he has been directed to a unique URL) to a "listener." This listener contains a proprietary communication protocol to enable the authentication web servers in the DMZ to communicate securely with the authentication application server and database server behind the firewall. The listener asks the applicant database behind the firewall to validate that the machine ID it has been given is legal, and not yet activated. If so, the listener tells the COM object to send a pop-up to the user, to collect the one-time activation key. If not, the activation process stops. De-Militarized Zone (DMZ) is from the military term for an area between two opponents, where fighting is prevented. DMZ Ethernets connect networks and computers controlled by different bodies. External DMZ Ethernets link regional networks with routers to internal networks. Internal DMZ Ethernets link local nodes with routers to the regional networks.

[0112] 6) If the key collected by the popup matches what is stored in the database for the user's account, the DLL proceeds to collect the user's hardware signature and sends them back to the data base. This hardware signature contains parameters including but not limited to CPU, hard disk and other hardware elements which may contain burnt in manufacturer's serial numbers or identifiers which can not be duplicated in any other machine or other distinguishing characteristics such as RAM, hard drive size, installed software, etc. If the key does not match, or the user does not answer within a set time limit, the activation process stops. After a set number of failed tries, the user's account is disabled.

[0113] 7) If the key matched, the DLL then returns a seed for an encrypted one-time password (OTP) for use during the next encounter. Another pop-up is sent to collect a personal password chosen by the user, which is known only to the user, and not stored anywhere.

[0114] 8) After the personal password has been collected, a configuration file containing, among other things, the OTP, which has just been exchanged, is encrypted. The account is then marked as active. On the next encounter, the one-time password just exchanged will be used as part of the authentication process. The key to opening the configuration file is the user's personal password together with parts of his computer's hardware.

[0115] Once the installation has been completed, the software components remaining on the home user's computer are the configuration file and the DLL containing the COM object. The COM object contains a self-validation routine, which lets it make sure that it has not been tampered with when it is loaded into memory, and a routine to establish a secure communication channel after it has made sure that it is intact. The secure communication channel is used to call a dynamically generated DLL from the server. In all future encounters, this dynamically generated DLL does most of the work in collecting information for the authentication process. The other components of the COM object are a locator, a profile manager and a payment method manager.

[0116] The locator ensures that the latest version of the software is installed, and locates the profile

manager and the payment method manager for a home user. The locator has two interfaces implemented via the agentclassId property and the agentCodeBase property. AgentClassId specifies which payment method manager and which profile manager to use. AgentCodeBase specifies which server holds the most updated version of the software, and compares what is installed to latest version. If the latest version is not installed, AgentCodeBase installs it automatically. This enables us to control what information is supplied to vendors while allowing vendors to code one standard line of code that never changes.

[0117] AgentClassId has five methods: get attribute, set attribute, set parameter, stop payment, and pay. Get attribute is a method to get non-sensitive information such as name, shipping information, etc.

[0118] Set attribute helps a browser page put this information into the user's computer. Set parameter helps configure the profile.

[0119] Stop payment lets the user stop in the middle of a transaction, once the pay method has been invoked.

[0120] Pay is responsible for establishing a secure communications channel, and returning the buyer's hardware signature and password on that channel.

[0121] The Payment Method Manager enables the choice of more than one payment option.

[0122] The profile manager allows different people to use the same hardware. One account may have multiple users, with multiple shipping addresses or billing addresses. A user may also choose to use billing information from a previously existing wallet such as Microsoft wallet, via the profile manager.

[0123] Transaction Cycle

[0124] Step 1--Customer Starts the Login Process at a Bank or Vendor

[0125] The first step occurs when the customer contacts a bank or vendor with vendor script installed and attempts to log in. This activates script, which was copied and pasted into the bank or vendor's e-commerce application.

[0126] Step 2--The Customer Contacts the TB

[0127] The script activates code, which contacts the DLL installed with the buyer's home software, and tries to load the COM object into memory. When the COM object is loaded into memory it runs an integrity test to make sure that it has not been tampered with. If the checksum is correct, it leaves the result in memory, so it can pass it later to the authentication server. Otherwise, it returns an error that disables the user's account and stops working.

[0128] If the COM object succeeds in verifying that it is intact, Pay attempts to contact a "listener" on the TB and establish a secure TCP/IP communication channel. Using RSA encryption, a shared secret key is now exchanged using a Diffie-Helman key exchange on this channel, and the encryption method switches to triple-DES. (In triple DES encryption, the encryption keys change several times during the transmission.)

[0129] The COM object then contacts the TB using the TB's public RSA key, passing to it the users account and machine IDs. The listener sends a request to validate the customer's account number and machine ID number to the application database, where the user's installation parameters are recorded. If they are valid, the listener then asks the COM object for an encrypted one-time password. This password is generated from a seed that was stored in a configuration file on the user's computer and in the TB's

user database during the last exchange between them. This one-time password is "unlocked" for use by the user's personal password, known only to him, and stored only in his mind, and by the CPU Id of his computer (When the transaction is an installation, and there has been no prior exchange, a first time activation key received from the owner system takes the place the place of the one-time password.)

[0130] If the numbers do not match, or if the user does not answer within a set time limit, the home user software sends back an error message, the account is temporarily disabled, and a log is created.

[0131] If the numbers match, the COM object knows that it is talking to the TB, since only the TB can decrypt messages sent with its public key, and the TB knows that it is talking to the right person since only he can "unlock" the one-time password.

[0132] Step 3--The TB Authenticates the Customer

[0133] Now that a secure channel exits, the listener on the TB sends a dynamically generated DLL to collect the home user's hardware signature information. This DLL is unique to each transaction. It returns signature in a string which is uniquely scrambled for each transaction and encrypted.

[0134] If all of the parameters match, the TB's authentication server can be sure it is talking to the correct customer, who is communicating from the correct computer. The TB returns a valid transaction ID to the customer, who passes it to the bank or vendor. In the bank model, the thread is closed, and an object on the server waits for the bank to inquire about the transaction. In the ISP or e-commerce model, the thread remains open, waiting for an order to issue a pop-up window to the user to validate purchase details for the transaction.

[0135] Step 4--The Bank or Vendor Contacts the TB to Verify the Transaction

[0136] Bank or Pure Authentication Model

[0137] The bank or other vendor passes customers account ID, machine ID, Listener ID, Provider ID and transaction ID to the TB. If these match what was stored in the database when the customer was authenticated, in the pure authentication model, the process ends here. A log-in transaction is validated and the customer continues on to carry out his transactions using the owners proprietary system, whatever that may be. Optionally, the TB may send the customer an SMS message notifying him of the transaction

[0138] ISP or E-commerce Models

[0139] In the ISP and other E-commerce models. payment details and credit availability must be validated in addition to user identity. In addition to the customer's account ID, machine ID, Listener ID, provider ID and transaction ID mentioned above, the Vendor passes the payment details (invoice number, invoice amount, currency) to the TB's authentication server. A new pop-up window is sent to the user on the secure channel previously established by Pay, asking him to authorize the invoice details. (As noted above, if the user does not answer within the set period of time, or rejects the transaction, the process is stopped and the thread dies). If the user accepts the transaction by clicking on the "Accept` button. TB's authentication server contacts a Payment server, and verifies that the user has credit available. If so, a transaction debiting the user and crediting the vendor is issued to the customer's chosen financial provider. Lastly, the TB notifies the vendor that the transaction is valid and the customer that a successful transaction has been completed. Optionally, the TB may send the customer an SMS message notifying him of the transaction.

[0140] With reference to FIG. 7, it can be seen that a typical purchasing session in this exemplary embodiment proceeds as follows:

[0141] a) User PC goes online and user points his browser to the Website of a Vendor server using any Web Browser Program; downloads files depicting merchandise for sale and selects merchandise to purchase which generates a purchase request to Vendor's server, all in a manner well known in the art.

[0142] b) Vendors server sends back to user PC an order page or pages which typically includes a transaction number, the value of the order, and asks for billing information, shipping information At some point, user is offered to indicate her desired method of payment and selects option button which designates the AA payment plan of the present invention, e.g "AA OPTION".

[0143] c) Selection of the "AA Option" generates a message back to Vendor's server which instructs the Vendor's server to forward a request to the Creditor's Toolbox to confirm that the user is (a) actually and actively online and trying to make this purchase, and (b) that the user has the necessary credit to make such a purchase.

[0144] a) Upon receipt of the request from Vendor's server, Toolbox immediately sends a transmission to the IP address provided by Vendor's server. The transmission includes files which (a) search for, decrypt and read the UID files in user's PC to see who it is, (if the PC is a machine registered in the system) and (b) which generate a Pop-up message on the registered user's browser to make sure that the transaction is desired by the AA system registered user. The message advises that a transaction having a particular value is being requested and asks for confirmation or rejection of the transaction. To reject the transaction, user can actively Reject by pressing a Reject button or simply by not responding within a predetermined default time.. To accept the transaction, the user must provide his user password and submit the form back to the Toolbox. The form is accompanied transparently by the fingerprint file containing the AID and other machine identifying information decrypted and extracted from user's PC by the transmission from the Toolbox.

[0145] a) If accepted by user, then Toolbox checks database to make sure user's credit limit is not exceeded and sends a coded confirmation to Vendor's server that the transaction is confirmed and will be paid for by Creditor on behalf of user. Vendor then sends HTML message to advise user that the identified transaction has been successfully processed.

[0146] As described above, if user either actively Rejects or fails to respond to the Pop-up message in a predetermined time period, for example, 2 minutes, the Pop-up message disappears and Toolbox advises Vendor's server that the transaction is not accepted. Optionally, provision can be made where user can label a tendered transaction as "suspicious" and reject an order with prejudice, thus alerting both Toolbox and Security Program Manager, and therefore Vendor, that some attempt was made to defraud Vendor.. Obviously, this knowledge can provide great benefits in aiding to track down cyber credit frauds and inhibit criminal activity.

[0147] In yet another exemplary embodiment, the Creditor server is also an ISP server, or at least they are at the same location and being serviced by the same modem basket. The Toolbox is still situated at that location as well. Thus, a bank which offers ISP services to it's on-line customers can also offer them the safety of the AA transaction system and method, which is carried out by the Toolbox right on the bank's/ISP's premises. The transaction continues as follows in the embodiment wherein the Toolbox is located at the ISP, hereinafter the ISP-Toolbox Model.

[0148] As was mentioned herein above, TB receives the encrypted password from the wallet if user accepted. TB can further have the ISP server verify that the session is still alive during the course of the transaction. This will validate the continued authenticity of the user. TB uses the encrypted password to change mark on transaction record from "not yet confirmed" to "Confirmed". The transaction record was assigned a unique ID number (UTID) which also serves as the Gatepost number and which is now sent to the vendor server, Vendor server receives the Gatepost number and forwards it to creditor or

payment server ("PS"), together with the amount to be paid and a vendor-assigned purchase transaction number.

[0149] For extra security, it is preferable that PS confirm the Gatepost with TB using the double handshake and priming routine with TB, similar to that performed between TB and users client PC. PS would check with the TB to verify that the session is still alive when TB responds, PS sends Gatepost received from Vendor together with transaction information. Optionally, when PS is registered as a participant in the security program, similar software agents and wallets could be installed on the PS so that TB can confirm PS identity after the handshake process using hardware fingerprints.

[0150] TB checks TB server database and if Gatepass and transaction information match the transaction record, then TB sends response to PS indicating that user has confirmed the desire to close the transaction and PS is authorized to charge User's account for the order. TB records on the transaction record that the payment request has been tendered and approved.

[0151] Physical Placement of TB in one exemplary embodiment, the TB is located at the physical site of the ISP, optimally connected to the phone or communication lines coming into the ISP server directly from users on one side of ISP server The TB is also connected to lines going out to the Internet (via the modem basket) from the ISP server. The TB does not interact directly with the ISP server. For the most part, it monitors incoming and outgoing traffic, waiting to take over those communications should a security related transaction be called for by a home user. The following scenario describes an exemplary embodiment of the process initiated when a request for a security related transaction is detected by the TB located at the ISP.. As will be further described below, in another exemplary embodiment, the Toolbox might not be located at the ISP but at the site of another credit provider.

[0152] a) User directs his browser to the URL of a vendor server and selects merchandise to purchase.

[0153] b) User is offered methods of payment and selects option button for "SECURITY PROGRAM MANAGER"or "AA PAY OPTION".

[0154] c) In an Autofetch process, an OnChange script handler in User's software prepares and sends request to central system administrator server for Session User Identity.

[0155] d) Central system administrator server redirects request to user's TB equipped ISP.

[0156] e) TB searches its files and returns user's identity

[0157] f) A *user form* is generated by *user's* computer and populated with user information including identity returned in step (e) from ISP TB.

[0158] g) The form is submitted, together with a challenge which is forwarded to the vendor server.

[0159] h) Vendor server runs a script that calls the central system administrator server's getGatePass.asp, thereby transmitting the Session User Identity.

[0160] i) The central system administrator server redirects the vendor server's call to the ISP.

[0161] j) The TB at the ISP receives the getGatePass.asp and runs a check of the user's authenticity as part of the vendor server's call to make the sure that is where the user really is logged in. If the authenticity fails, the vendor server receives a rejection notification from the ISP server and the transaction is terminated.

[0162] k) If the IP test succeeds (i.e. the user really is who they claim to be) then the ISP challenges the

home listener.

[0163] FIG. 10 illustrates a situation where client 204 is located remotely from his PC 212, for example driving his car 206. An intruder 208 has gained access to his PC 212, and has fraudulently attempted a secure transaction. The AA communicates a message accordingly to client 204 via the Internet 220. The client can be remotely contacted, for example, through his cell phone 230, his pager 240 or his PDA 210. Client 204 is shown receiving the message through his cell phone 230

[0164] FIG. 11 illustrates client 302 sending a simultaneous message 304 to AA 306 and vendor 308.

[0165] The fingerprint mechanism of the present invention can be adapted for use to ensure ownership rights in downloaded copyrighted material, such as content files which includes MP3 music files, e-books, graphic files, and the like. In the event a content file is to be purchased by a user, for example, if a user orders an MP3 file, the user is directed to a URL address for downloading the file The digital fingerprint provided by the smart DLL in the user's PC is incorporated into code in the content file itself. Thus, the file is only downloadable if the fingerprint information encoded into the file matches that of the user's PC. Additionally, the content file can be encoded to limit how and where the downloaded file can be accessed and operated. The encoding can determine whether or not the file can be transferred to a limited number of other PC. Alternatively, the ID is associated with a diskette, as described herein above, and may be transferred to a limited number of PC's or perhaps only to one other MP3 player (or PDAs in the case of an e-book).

[0166] It will be appreciated that the preferred embodiments described above are cited by way of example, and that the present invention is not limited to what has been particularly shown and described hereinabove. Rather, the scope of the present invention includes both combinations and sub-combinations of the various features described hereinabove, as well as variations and modifications thereof which would occur to persons skilled in the art upon reading the foregoing description, and which are not disclosed in the prior art.

* * * * *

-->